

Docket No.: 67471-037

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 20277
	:	
Takio YAMASHITA	:	Confirmation Number:
	:	
Serial No.:	:	Group Art Unit:
	:	
Filed: March 17, 2004	:	Examiner:
	:	
For:	:	DEBUG SYSTEM, MICROPROCESSOR, AND DEBUGGER

**CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Mail Stop CPD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicant hereby claim the priority of:

Japanese Patent Application No. JP 2003-076145, filed on March 19, 2003.

A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY


Michael E. Fogarty
Registration No. 36,139

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 MEF:gav
Facsimile: (202) 756-8087
Date: March 17, 2004

67471-037
Takio YAMASHITA
March 17, 2004

日本国特許庁 *McDermott, Will & Emery*
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 3月19日
Date of Application:

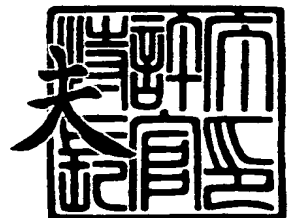
出願番号 特願2003-076145
Application Number:
[ST. 10/C]: [JP 2003-076145]

出願人 松下電器産業株式会社
Applicant(s):

2003年12月17日

特許庁長官
Commissioner,
Japan Patent Office

今井 康



出証番号 出証特2003-3104706

【書類名】 特許願

【整理番号】 5037730155

【提出日】 平成15年 3月19日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 12/14

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社
会社内

【氏名】 山下 太紀夫

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100090446

【弁理士】

【氏名又は名称】 中島 司朗

【手数料の表示】

【予納台帳番号】 014823

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9003742

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 デバッグシステム、マイクロプロセッサ及びデバッガ

【特許請求の範囲】

【請求項 1】 外部に秘匿するプログラム情報を記憶しているマイクロプロセッサと、前記マイクロプロセッサと接続され、前記マイクロプロセッサの動作をデバッグするために用いられるホストコンピュータとから構成されるデバッグシステムであって、

前記マイクロプロセッサは、

前記プログラム情報をセキュアに扱うために用いられる鍵情報を記憶する為の領域を備える一度だけ書き込みが可能な不揮発性メモリと、

前記不揮発性メモリが鍵情報を記憶していない場合に、前記ホストコンピュータから鍵情報を受け取り、受け取った鍵情報を前記不揮発性メモリに書き込む書込手段と、

前記不揮発性メモリが記憶している鍵情報を用いて、前記ホストコンピュータとの間で前記プログラム情報をセキュアに伝送する第 1 伝送手段とを備え、

前記ホストコンピュータは、

利用者から鍵情報の入力を受け付ける受付手段と、

前記鍵情報を内部に記憶すると共に、前記マイクロプロセッサへ送出する送出手段と、

記憶している前記鍵情報を用いて、前記マイクロプロセッサとの間で前記プログラム情報をセキュアに伝送する第 2 伝送手段とを備える

ことを特徴とするデバッグシステム。

【請求項 2】 デバッグするために用いられるホストコンピュータと接続され、外部に秘匿するプログラム情報を記憶しているマイクロプロセッサであって、

プログラム、データ又はプログラム及びデータを示す前記プログラム情報を記憶しているプログラム情報記憶手段と、

前記プログラム情報を読み出し、読み出したプログラム情報に従って動作する実行手段と、

前記プログラム情報をセキュアに扱うために用いられる鍵情報を記憶する為の

領域を備える一度だけ書き込みが可能な不揮発性メモリと、

前記不揮発性メモリが鍵情報を記憶していない場合に、前記ホストコンピュータから鍵情報を受け取り、受け取った鍵情報を前記不揮発性メモリに書き込む書込手段と、

前記不揮発性メモリが記憶している鍵情報を用いて、前記ホストコンピュータとの間で前記プログラム情報をセキュアに伝送する伝送手段とを備える

ことを特徴とするマイクロプロセッサ。

【請求項 3】 前記不揮発性メモリは、鍵情報が書き込み済みか否かを示すフラグ情報を記憶しており、

前記伝送手段は、前記フラグ情報を読み出し、読み出した前記フラグ情報が前記不揮発性メモリに鍵情報が書き込まれていないことを示す場合に、前記ホストコンピュータから鍵情報を受け付け、受け付けた鍵情報を前記不揮発性メモリに書き込む

ことを特徴とする請求項 2 に記載のマイクロプロセッサ。

【請求項 4】 前記伝送手段は、

前記不揮発性メモリに記憶されている鍵情報を用いて、前記プログラム情報を暗号化する暗号化部と、

暗号化されたプログラム情報を出力する出力部とを含む

ことを特徴とする請求項 3 に記載のマイクロプロセッサ。

【請求項 5】 前記プログラム情報記憶手段は、前記プログラム、データ又はプログラム及びデータが鍵情報を用いて暗号化されて生成されたプログラム情報を記憶しており、

前記実行手段は、前記不揮発性メモリから鍵情報を読み出し、読み出した鍵情報を用いて、プログラム情報を復号してプログラム、データ又はプログラム及びデータを生成し、生成したプログラム、データ又はプログラム及びデータに従って動作し、

前記伝送手段は、プログラム、データ又はプログラム及びデータが暗号化されて生成されたプログラム情報を伝送する

ことを特徴とする請求項 3 に記載のマイクロプロセッサ。

【請求項 6】 前記実行手段は、更に、動作の結果生成された生成データを、鍵情報を用いて暗号化し、暗号化された生成データを前記プログラム情報記憶手段に書き込む

ことを特徴とする請求項 5 に記載のマイクロプロセッサ。

【請求項 7】 前記プログラム情報記憶手段は、前記プログラムのみが鍵情報を用いて暗号化された暗号化プログラムを含むプログラム情報を記憶しており、前記プログラム情報記憶手段は、前記外部装置との通信経路を備える

ことを特徴とする請求項 5 に記載のマイクロプロセッサ。

【請求項 8】 前記鍵情報は 1 以上の部分鍵情報から構成され、前記プログラムは、複数の部分プログラムから構成され、各部分プログラムは、前記 1 以上の部分鍵情報の何れかに対応しており、

前記プログラム情報記憶手段は、複数の部分プログラムが、対応する部分鍵情報を用いて暗号化された暗号化部分プログラムを含むプログラム情報を記憶しており、

前記実行手段は、前記不揮発性メモリから部分鍵情報を読み出し、読み出した部分鍵情報に対応する 1 以上の暗号化部分プログラムをプログラム情報記憶手段から読み出し、読み出した 1 以上の暗号化部分プログラムを、前記部分鍵情報を用いて復号して部分プログラムを生成し、生成した部分プログラムに従って動作する

ことを特徴とする請求項 5 に記載のマイクロプロセッサ。

【請求項 9】 前記伝送手段は、さらに、前記ホストコンピュータからの要求に応じて、前記出力部における暗号化されたプログラム情報の出力を抑制する抑制部を含む

ことを特徴とする請求項 4 に記載のマイクロプロセッサ。

【請求項 10】 前記伝送手段は、さらに、鍵情報に係る情報で、前記出力部における暗号化されたプログラム情報の出力の抑制を示す抑制条件を記憶している抑制条件記憶部と、

前記ホストコンピュータから受け付けた前記鍵情報が、前記抑制条件を満たす場合に、前記出力部における前記出力を抑制する抑制部とを含む

ことを特徴とする請求項 4 に記載のマイクロプロセッサ。

【請求項 1 1】 前記不揮発性メモリは、鍵情報が書き込み済みか否かを示すフラグ情報を記憶しており、

前記伝送手段は、前記フラグ情報を読み出し、読み出したフラグ情報が前記不揮発性メモリに鍵情報が書き込まれていないことを示す場合に、前記プログラム情報記憶手段から前記プログラム情報を読み出し、読み出したプログラム情報を出力し、読み出したフラグ情報が前記不揮発性メモリに鍵情報が書き込まれていることを示す場合に、前記プログラム情報記憶手段から前記プログラム情報を読み出し、読み出したプログラム情報を前記鍵情報で暗号化し、暗号化されたプログラム情報を出力する

ことを特徴とする請求項 2 に記載のマイクロプロセッサ。

【請求項 1 2】 前記マイクロプロセッサは、更に、キャッシュメモリを備え、

前記プログラム情報記憶手段は、前記プログラム、データ又はプログラム及びデータが鍵情報を用いて暗号化されて生成されたプログラム情報を記憶しており、

前記実行手段は、前記不揮発性メモリから鍵情報を読み出し、読み出した鍵情報を用いて、プログラム情報を復号してプログラム、データ又はプログラム及びデータを生成し、生成した前記プログラム、データ又はプログラム及びデータを前記キャッシュメモリに書き込み、前記実行手段の実行速度に応じて前記キャッシュメモリから前記プログラム、データ又はプログラム及びデータを読み出し、読み出したプログラム、データ又はプログラム及びデータに従って動作し、

前記伝送手段は、プログラム、データ又はプログラム及びデータが暗号化されて生成されたプログラム情報を伝送する

ことを特徴とする請求項 3 に記載のマイクロプロセッサ。

【請求項 1 3】 外部に秘匿するプログラム情報を記憶しているマイクロプロセッサと接続され、前記マイクロプロセッサの動作をデバッグするホストコンピュータであって、

利用者から鍵情報の入力を受け付ける受付手段と、

前記鍵情報を、内部に記憶すると共に前記マイクロプロセッサへ送出する送出手段と、

記憶している前記鍵情報を用いて、前記マイクロプロセッサとの間で前記プログラム情報をセキュアに伝送する伝送手段とを備える

ことを特徴とするホストコンピュータ。

【請求項 14】 前記伝送手段は、

前記マイクロプロセッサから、前記鍵情報を用いて暗号化されたプログラム情報を受け取るプログラム情報受取部と、

前記暗号化されたプログラム情報に、記憶している前記鍵情報を用いて復号する復号部と、

前記復号部が復号したプログラム情報を表示する表示部とを備える

ことを特徴とする請求項 13 に記載のホストコンピュータ。

【請求項 15】 前記伝送手段は、更に、

利用者から、プログラム、データ又はプログラム及びデータを示すプログラム情報の入力を受け付けるプログラム情報入力部と、

受け付けた前記プログラム情報に、記憶している前記鍵情報を用いて暗号化する暗号部と、

前記暗号部が暗号化したプログラム情報を前記マイクロプロセッサへ出力する出力部とを備える

ことを特徴とする請求項 14 に記載のホストコンピュータ。

【請求項 16】 前記ホストコンピュータは、更に、

ソースプログラムを記憶している記憶手段と、

前記ソースプログラムを変換してプログラムを示すプログラム情報を生成する変換手段と、

前記プログラム情報に、前記鍵情報を用いて暗号化する暗号化手段とを備え、

前記伝送手段は、前記暗号化手段が暗号化したプログラム情報を前記マイクロプロセッサへ伝送する

ことを特徴とする請求項 14 に記載のホストコンピュータ。

【請求項 17】 前記伝送手段は、さらに、

鍵情報に係る情報で、前記マイクロプロセッサとの間での前記暗号化されたプログラム情報の伝送の停止を示す停止条件を記憶している停止条件記憶部と、

前記入力手段が受け付けた前記鍵情報が、前記停止条件を満たす場合に、前記マイクロプロセッサに対して、前記暗号化されたプログラム情報の出力を抑制することを示す要求 部を出力する抑制要求出力部とを含む

ことを特徴とする請求項 14 に記載のホストコンピュータ。

【請求項 18】 外部に秘匿するプログラム情報を記憶しているマイクロプロセッサと接続されたリードライト装置であって、

利用者から鍵情報の入力を受け付ける受付手段と、

前記鍵情報を内部に記憶すると共に前記マイクロプロセッサへ送出する送出手段と、

記憶している前記鍵情報を用いて、前記マイクロプロセッサとの間で前記プログラム情報をセキュアに伝送する伝送手段とを備える

ことを特徴とするリードライト装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、マイクロプロセッサ及び前記マイクロプロセッサをデバッグする技術に関する。

【0002】

【従来の技術】

昨今、ICチップを搭載したICカードが課金処理を扱うシステムで用いられるようになってきている。ICチップは、マイクロプロセッサ、ROM、RAMなどを備える微小なコンピュータシステムである。前記ROMには、制御用コンピュータプログラムが格納されており、前記マイクロプロセッサは制御用コンピュータプログラムを実行することにより、ICカードの課金処理を制御する。

【0003】

一方で、マイクロプロセッサは、設計後及び出荷後のデバッグを可能にするために、デバッグインターフェースを搭載している。デバッグとは、デバッグユニ

ットと接続されたホストパーソナルコンピュータ（以下「ホストPC」と言う）上で動作するデバッガが、当該マイクロプロセッサ内部のメモリに格納された命令又はデータを抽出してホストPC上に表示すること、及び、ホストPC上で入力された命令又はデータをマイクロプロセッサのメモリに書き込むことにより、プログラムのバグを見つけて修正することである。

【0004】

この様に、デバッグインターフェースを搭載しているマイクロプロセッサが、課金情報を扱うシステムで用いられるICカードに搭載されると、悪意のある解析者に内部の命令及びデータを不正に解析、改竄される危険性があるため、このようなシステムで用いるマイクロプロセッサには、命令及びデータを解析、改竄されるのを防止するための高いセキュリティが要求される。

【0005】

そこで、特許文献1によると、実行プログラムを内蔵したROMと前記ROMに前記実行プログラムを書き込む入出力装置と前記ROMから前記実行プログラムを読み出す半導体プロセッサとから構成される情報保護システムであって、暗号化した実行プログラムをROMに書き込み、暗号化された実行プログラムを前記ROMから読み出し、復号する技術が開示されている。

【0006】

また、特許文献2によると、ROMに記録された情報を、外部に設けられたデバッグツールによる不正アクセスから保護する情報処理装置であって、ユーザにより個別に設定可能なセキュリティ解除プログラムを含み、外部に設けられたエミュレータによる不正アクセスから保護すべき情報を記憶するメモリと、前記エミュレータに接続されて、前記エミュレータと当該情報処理装置との間でデバッグに必要な信号の入出力制御を行い、前記情報処理装置のデバッグをサポートするオンチップデバッグ回路とを備え、電源投入時に前記情報処理装置をリセットするパワーオンリセット信号を受けて、前記オンチップデバッグ回路の機能を無効化してセキュリティを設定し、前記エミュレータによる前記メモリが記憶している前記情報の読み出しを禁止し、セキュリティ指定ビットと当該セキュリティ指定ビットのリセットをイネーブルとするイネーブルコードとを受けて、前記オ

ンチップデバッグ回路の機能を有効化してセキュリティを解除し、前記エミュレータによる、前記情報の読み出しを可能にする情報処理装置に関する技術が開示されている。

【0007】

上記の様に、内部情報を保護するためにマイクロプロセッサに暗号化回路を設け、内部情報を暗号化して外部へ出力することが行われている。マイクロプロセッサは、設計時に設定されたキーコードを保持しており、このキーコードを用いて命令及びデータの暗号化を行う。ホストPC上で動作するデバッガは、復号化回路を備え、前記マイクロプロセッサから暗号化された命令及びデータを受信し、前記キーコードの入力を受け付けて命令及びデータを復号する。従って、前記キーコードを知る者のみが正しく復号された命令及びデータを得てデバッグを行うことが出来る。

【0008】

【特許文献1】

特開 2000-357085 号公報

【0009】

【特許文献2】

特開 2000-347942 号公報

【0010】

【発明が解決しようとする課題】

しかしながら、上記のマイクロプロセッサは、設計時にキーコードを書き込む為、当該キーコードはマイクロプロセッサ設計者やデバッガ設計者等のシステム開発者には既知である。課金情報を扱うシステムで用いられるICカードを例に考えると、マイクロプロセッサ製造者とICカード製造者とICカード供給者とはそれぞれ異なる。マイクロプロセッサ製造者及びICカード製造者は当該システムの利用者なり得るため、マイクロプロセッサにデバッグユニットを接続して内部情報を解読、改竄されかねないという問題がある。

【0011】

本発明は、上記問題点に鑑みなされたものであって、マイクロプロセッサのデ

バッグと内部情報のセキュリティの確保とを両立できるマイクロプロセッサ、デバッグ及びデバッグシステムを提供することを目的とする。

【0012】

【課題を解決するための手段】

上記目的を達成するために、本発明は、外部に秘匿するプログラム情報を記憶しているマイクロプロセッサと、前記マイクロプロセッサと接続され、前記マイクロプロセッサの動作をデバッグするために用いられるホストコンピュータとから構成されるデバッグシステムである。

【0013】

前記マイクロプロセッサは、前記プログラム情報をセキュアに扱うために用いられる鍵情報を記憶する為の領域を備える一度だけ書き込みが可能な不揮発性メモリと、前記不揮発性メモリが鍵情報を記憶していない場合に、前記ホストコンピュータから鍵情報を受け取り、受け取った鍵情報を前記不揮発性メモリに書き込む書込手段と、前記不揮発性メモリが記憶している鍵情報を用いて、前記ホストコンピュータとの間で前記プログラム情報をセキュアに伝送する第1伝送手段とを備える。

【0014】

前記ホストコンピュータは、利用者から鍵情報の入力を受け付ける受付手段と、前記鍵情報を内部に記憶すると共に、前記マイクロプロセッサへ送出的送手段と、記憶している前記鍵情報を用いて、前記マイクロプロセッサとの間で前記プログラム情報をセキュアに伝送する第2伝送手段とを備える。

また、本発明は、デバッグするために用いられるホストコンピュータと接続され、外部に秘匿するプログラム情報を記憶しているマイクロプロセッサである。前記マイクロプロセッサは、プログラム、データ又はプログラム及びデータを示す前記プログラム情報を記憶しているプログラム情報記憶手段と、前記プログラム情報を読み出し、読み出したプログラム情報に従って動作する実行手段と、前記プログラム情報をセキュアに扱うために用いられる鍵情報を記憶する為の領域を備える一度だけ書き込みが可能な不揮発性メモリと、前記不揮発性メモリが鍵情報を記憶していない場合に、前記ホストコンピュータから鍵情報を受け取り、

受け取った鍵情報を前記不揮発性メモリに書き込む書込手段と、前記不揮発性メモリが記憶している鍵情報を用いて、前記ホストコンピュータとの間で前記プログラム情報をセキュアに伝送する伝送手段とを備えることを特徴とする。

【0015】

ここで、前記不揮発性メモリは、鍵情報が書き込み済みか否かを示すフラグ情報を記憶しており、前記伝送手段は、前記フラグ情報を読み出し、読み出した前記フラグ情報が前記不揮発性メモリに鍵情報が書き込まれていないことを示す場合に、前記ホストコンピュータから鍵情報を受け付け、受け付けた鍵情報を前記不揮発性メモリに書き込むことを特徴とする。

【0016】

ここで、前記伝送手段は、前記不揮発性メモリに記憶されている鍵情報を用いて、前記プログラム情報を暗号化する暗号化部と、暗号化されたプログラム情報を出力する出力部とを含むことを特徴とする。

また、前記プログラム情報記憶手段は、前記プログラム、データ又はプログラム及びデータが鍵情報を用いて暗号化されて生成されたプログラム情報を記憶しており、前記実行手段は、前記不揮発性メモリから鍵情報を読み出し、読み出した鍵情報を用いて、プログラム情報を復号してプログラム、データ又はプログラム及びデータを生成し、生成したプログラム、データ又はプログラム及びデータに従って動作し、前記伝送手段は、プログラム、データ又はプログラム及びデータが暗号化されて生成されたプログラム情報を伝送することを特徴とする。

【0017】

ここで、前記実行手段は、更に、動作の結果生成された生成データを、鍵情報を用いて暗号化し、暗号化された生成データを前記プログラム情報記憶手段に書き込むことを特徴とする。

ここで、前記プログラム情報記憶手段は、前記プログラムのみが鍵情報を用いて暗号化された暗号化プログラムを含むプログラム情報を記憶しており、前記プログラム情報記憶手段は、前記外部装置との通信経路を備えることを特徴とする。

【0018】

また、前記鍵情報は 1 以上の部分鍵情報から構成され、前記プログラムは、複数の部分プログラムから構成され、各部分プログラムは、前記 1 以上の部分鍵情報の何れかに対応しており、前記プログラム情報記憶手段は、複数の部分プログラムが、対応する部分鍵情報を用いて暗号化された暗号化部分プログラムを含むプログラム情報を記憶しており、前記実行手段は、前記不揮発性メモリから部分鍵情報を読み出し、読み出した部分鍵情報に対応する 1 以上の暗号化部分プログラムをプログラム情報記憶手段から読み出し、読み出した 1 以上の暗号化部分プログラムを、前記部分鍵情報を用いて復号して部分プログラムを生成し、生成した部分プログラムに従って動作することを特徴とする。

【0019】

また、前記伝送手段は、さらに、前記ホストコンピュータからの要求に応じて、前記出力部における暗号化されたプログラム情報の出力を抑制する抑制部を含むことを特徴とする。

また、前記伝送手段は、さらに、鍵情報に係る情報で、前記出力部における暗号化されたプログラム情報の出力の抑制を示す抑制条件を記憶している抑制条件記憶部と、前記ホストコンピュータから受け付けた前記鍵情報が、前記抑制条件を満たす場合に、前記出力部における前記出力を抑制する抑制部とを含むことを特徴とする。

【0020】

また、前記不揮発性メモリは、鍵情報が書き込み済みか否かを示すフラグ情報を記憶しており、前記伝送手段は、前記フラグ情報を読み出し、読み出したフラグ情報が前記不揮発性メモリに鍵情報が書き込まれていないことを示す場合に、前記プログラム情報記憶手段から前記プログラム情報を読み出し、読み出したプログラム情報を出力し、読み出したフラグ情報が前記不揮発性メモリに鍵情報が書き込まれていることを示す場合に、前記プログラム情報記憶手段から前記プログラム情報を読み出し、読み出したプログラム情報を前記鍵情報で暗号化し、暗号化されたプログラム情報を出力することを特徴とする。

【0021】

前記マイクロプロセッサは、更に、キャッシュメモリを備え、前記プログラム

情報記憶手段は、前記プログラム、データ又はプログラム及びデータが鍵情報を用いて暗号化されて生成されたプログラム情報を記憶しており、前記実行手段は、前記不揮発性メモリから鍵情報を読み出し、読み出した鍵情報を用いて、プログラム情報を復号してプログラム、データ又はプログラム及びデータを生成し、生成した前記プログラム、データ又はプログラム及びデータを前記キャッシュメモリに書き込み、前記実行手段の実行速度に応じて前記キャッシュメモリから前記プログラム、データ又はプログラム及びデータを読み出し、読み出したプログラム、データ又はプログラム及びデータに従って動作し、前記伝送手段は、プログラム、データ又はプログラム及びデータが暗号化されて生成されたプログラム情報を伝送することを特徴とする。

【0022】

また、本発明は、外部に秘匿するプログラム情報を記憶しているマイクロプロセッサと接続され、前記マイクロプロセッサの動作をデバッグするホストコンピュータである。前記ホストコンピュータは、利用者から鍵情報の入力を受け付ける受付手段と、前記鍵情報を、内部に記憶すると共に前記マイクロプロセッサへ送出する送出手段と、記憶している前記鍵情報を用いて、前記マイクロプロセッサとの間で前記プログラム情報をセキュアに伝送する伝送手段とを備えることを特徴とする。

【0023】

ここで、前記伝送手段は、前記マイクロプロセッサから、前記鍵情報を用いて暗号化されたプログラム情報を受け取るプログラム情報受取部と、前記暗号化されたプログラム情報に、記憶している前記鍵情報を用いて復号する復号部と、前記復号部が復号したプログラム情報を表示する表示部とを備えることを特徴とする。

【0024】

ここで、前記伝送手段は、更に、利用者から、プログラム、データ又はプログラム及びデータを示すプログラム情報の入力を受け付けるプログラム情報入力部と、受け付けた前記プログラム情報に、記憶している前記鍵情報を用いて暗号化する暗号部と、前記暗号部が暗号化したプログラム情報を前記マイクロプロセッ

サへ出力する出力部とを備えることを特徴とする。

【0025】

前記ホストコンピュータは、更に、ソースプログラムを記憶している記憶手段と、前記ソースプログラムを変換してプログラムを示すプログラム情報を生成する変換手段と、前記プログラム情報に、前記鍵情報を用いて暗号化する暗号化手段とを備え、前記伝送手段は、前記暗号化手段が暗号化したプログラム情報を前記マイクロプロセッサへ伝送することを特徴とする。

【0026】

ここで、前記伝送手段は、さらに、鍵情報に係る情報で、前記マイクロプロセッサとの間の前記暗号化されたプログラム情報の伝送の停止を示す停止条件を記憶している停止条件記憶部と、前記入力手段が受け付けた前記鍵情報が、前記停止条件を満たす場合に、前記マイクロプロセッサに対して、前記暗号化されたプログラム情報の出力を抑制することを示す要求を出力する抑制要求出力部とを含むことを特徴とする。

【0027】

また、本発明は、外部に秘匿するプログラム情報を記憶しているマイクロプロセッサと接続されたリードライト装置である。前記リードライト装置は、利用者から鍵情報の入力を受け付ける受付手段と、前記鍵情報を内部に記憶すると共に前記マイクロプロセッサへ送出する送出手段と、記憶している前記鍵情報を用いて、前記マイクロプロセッサとの間で前記プログラム情報をセキュアに伝送する伝送手段とを備えることを特徴とする。

【0028】

【発明の実施の形態】

1. 第1の実施の形態

本発明に係る第1の実施の形態として、デバッグシステム1について図面を参照して説明する。

<構成>

ここでは、デバッグシステム1の構成について説明する。デバッグシステム1は、マイクロプロセッサ10、デバッグユニット11、ホストPC12及び外部

メモリ 13 から構成される。

【0029】

マイクロプロセッサ 10 と外部メモリ 13 とは、ユーザが開発する IC カードの基板上に搭載されており、外部バスを介して互いに接続されている。また、デバッグユニット 11 は、ケーブルを介してマイクロプロセッサ 10 及びホスト PC 12 と接続されている。ここで、外部メモリ 13 には、命令及びデータから成るコンピュータプログラムが記憶されており、当該コンピュータプログラムは、マイクロプロセッサ 10 により実行される。

【0030】

以下では、マイクロプロセッサ 10 及びホスト PC 12 について詳しく説明する。

(マイクロプロセッサ 10)

図 1 は、マイクロプロセッサ 10 の構成を示すブロック図である。同図に示す様に、マイクロプロセッサ 10 は、命令メモリ 101、命令実行ユニット 102、データメモリ 103、データ処理ユニット 104、不揮発性メモリ 105、暗号化回路 106、デバッグインターフェース 107 及びバスコントローラ 108 から構成される。

【0031】

命令メモリ 101 は、具体的には RAM (Random Access Memory) 及び ROM (Read Only Memory) であって命令を記憶している。命令メモリ 101 は、バスを介して命令実行ユニット 102 と接続されている。更に、命令メモリ 101 は、バスを介して暗号化回路 106 と接続されており、デバッグユニット 11 を介して接続されたホスト PC 12 上で動作するデバッガの要求を受けて、記憶している命令を暗号化回路 106 へ出力する。また、命令メモリ 101 は、暗号化回路 106 から出力される命令を受け取り記憶する。

【0032】

命令実行ユニット 102 は、バスを介して命令メモリ 101 と接続されており、命令メモリ 101 が記憶している命令を読み出し、解釈し、実行する。更に、命令実行ユニット 102 は、バスコントローラ 108 及び外部バスを介して外部

メモリ 13 と接続されており、外部メモリ 13 が記憶している命令を、バスコントローラ 108 を介して読み出し、解釈し、実行する。

【0033】

データメモリ 103 は、具体的には ROM 又は RAM であってデータを記憶している。データメモリ 103 は、バスを介してデータ処理ユニット 104 に接続されており、データ処理ユニット 104 からの要求を受けて、データ処理ユニット 104 へデータを出力する。データメモリ 103 は、データ処理ユニット 104 が出力する演算結果を受け取り記憶する。更に、データメモリ 103 は、バスを介して暗号化回路 106 と接続されており、デバッグユニット 11 を介して接続されたホスト PC 12 上で動作するデバッガの要求を受けて、記憶しているデータを暗号化回路 106 へ出力する。また、データメモリ 103 は、暗号化回路 106 から出力されるデータを受け取り記憶する。

【0034】

データ処理ユニット 104 は、バスを介してデータメモリ 103 と接続されており、データメモリ 103 からデータを読み出し、読み出したデータに演算処理を施し、演算結果をデータメモリ 103 に書き込む。更に、データ処理ユニット 104 は、バス及びバスコントローラ 108 を介して外部メモリ 13 と接続されており、外部メモリ 13 が記憶しているデータを、バスコントローラ 108 を介して読み出し、読み出したデータに演算処理を施し、演算結果を外部メモリ 13 に書き込む。

【0035】

不揮発性メモリ 105 は、キーコードを記憶する領域と判定フラグを記憶する領域とを備え、キーコードと判定フラグとが書き込まれると、それらを所定の領域に記憶する。キーコードは、暗号化回路 106 による命令の暗号化及びデータの暗号化に用いられる暗号鍵であって、一度だけ書き込みが可能であり、読み出し及び書き換えが出来ない。判定フラグは、キーコードが不揮発性メモリ 105 に書き込み済みか否かを判定するために用いるフラグであって、キーコードが不揮発性メモリ 105 に書き込まれると、判定フラグが不揮発性メモリ 105 に書き込まれる。また、判定フラグは一度だけ書き込みが可能であり、書き換えが出

来ない。

【0036】

暗号化回路106は、命令メモリ101に記憶されている命令をデバッグインターフェース107及びデバッグユニット11を介してホストPC12が読み出すとき、また、データメモリ103に記憶されているデータをデバッグインターフェース107及びデバッグユニット11を介してホストPC12が読み出すときに命令及びデータを暗号化するための回路である。暗号化回路106は、不揮発性メモリ105が記憶しているキーコードを暗号鍵として用いて命令メモリ101に記憶されている命令及びデータメモリに記憶されているデータに、暗号アルゴリズムE₁を施し暗号化命令及び暗号化データを生成する。ここで暗号アルゴリズムE₁は、例えばDES (Data Encryption Standard) である。暗号化回路106は、生成した暗号化命令及び暗号化データをデバッグインターフェース107及びデバッグユニット11を介してホストPC12へ出力する。

【0037】

デバッグインターフェース107は、デバッグ端子を含むインターフェースであって、暗号化回路106とデバッグユニット11、及び、不揮発性メモリ105とデバッグユニット11を接続する。

更に、デバッグインターフェース107は、デバッグユニット11を介してホストPC12から「命令表示」を示す信号を受け取ると、命令メモリ101から命令を抽出し、抽出した命令を暗号化回路106へ出力する。また、「データ表示」を示す信号を受け取ると、データメモリ103からデータを抽出し、抽出したデータを暗号化回路106へ出力する。また、デバッグインターフェース107は、デバッグユニット11を介してホストPC12から命令を受け取ると、受け取った命令を、暗号化回路106を介して命令メモリ101へ書き込む。このとき、デバッグインターフェース107は、暗号化回路106に対して命令に暗号化処理を施さずに命令メモリ101へ書き込むことを指示する。データを受け取ると、受け取ったデータを、暗号化回路106を介してデータメモリ103へ書き込む。このとき、デバッグインターフェース107は、暗号化回路106に対してデータに暗号化処理を施さずにデータメモリ103へ書き込むことを指示

する。暗号化回路 106 はデータに対して暗号化処理を行わずに、データメモリ 103 へデータを書き込む。

【0038】

バスコントローラ 108 は、マイクロプロセッサ 10 の外部に設けられた外部メモリ 13 と命令実行ユニット 102、及び外部メモリ 13 とデータ処理ユニット 104 との間で情報の受け渡しをする。

(ホスト PC 12)

ホスト PC 12 は、マイクロプロセッサ 10 に対応するデバグが動作するコンピュータシステムであって、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるパーソナルコンピュータである。前記ハードディスクユニットには、デバグを含む各種のコンピュータプログラムが記憶されている。

【0039】

図 2 は、ホスト PC 12 の機能を示す機能ブロック図である。同図に示す様に、ホスト PC 12 は、表示部 121 とデバグ部 122 とを備える。デバグ部 122 は、前記ハードディスクユニットに記憶されているデバグが前記マイクロプロセッサにより実行されるとききの動作を機能的に示すものであり、デバグ部 122 は、キーコード入力部 123、コマンド入力部 124、復号部 125 及び命令・データ入力部 126 を含む。

【0040】

表示部 121 は、ディスプレイユニットを含み、デバグ部 122 が出力する画面データをディスプレイに表示する。また、表示部 121 は、キーコードの入力を受け付けるための画面がディスプレイに表示されている状態において、キーコード入力部 123 が受け付けた内容を前記画面上に表示する。同様に、表示部 121 は、コマンドの入力を受け付けるための画面がディスプレイに表示されている状態において、コマンド入力部 124 が受け付けた内容を前記画面上に表示する。同様に、表示部 121 は、命令の入力を受け付けるための画面がディスプレイに表示されている状態において、命令・データ入力部 126 が受け付けた内容を前記画面上に表示する。同様に、データの入力を受け付けるための画面がデ

ディスプレイに表示されている状態において、命令・データ入力部 126 が受け付けた内容を前記画面上に表示する。

【0041】

キーコード入力部 123 は、キーコードの入力を受け付けるための画面の生成に用いる画面情報を表示部 121 へ出力する。キーコード入力部 123 は、表示部 121 にキーコードの入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボード及びマウスを介したキーコードの入力を受け付ける。キーコード入力部 123 は、キーコードを受け付けると、受け付けたキーコードを記憶する。更に、キーコード入力部 123 は、デバッグユニット 11 及びマイクロプロセッサ 10 のデバッグインターフェース 107 を介して、不揮発性メモリ 105 から判定フラグを読み、不揮発性メモリ 105 にキーコードが書き込み済みか否か判断する。書き込み済みでない場合、キーコード入力部 123 は、キーコードを、デバッグユニット 11 及びデバッグインターフェース 107 を介して不揮発性メモリ 105 に送出する。キーコード入力部 123 は、デバッグ部 122 の動作が終了すると、記憶したキーコードを破棄する。

【0042】

コマンド入力部 124 は、コマンドの入力を受け付けるための画面の生成に用いる画面情報を表示部 121 へ出力する。コマンド入力部 124 は、表示部 121 にコマンドの入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボード及びマウスを介したコマンドの入力を受け付ける。更に、コマンド入力部 124 は、受け付けたコマンドを判断する。コマンドが「命令表示」であれば、コマンド入力部 124 は、「命令表示」を示す信号をデバッグユニット 11 を介してデバッグインターフェース 107 へ送出する。コマンドが「命令書込み」であれば、コマンドに対応する信号を命令・データ入力部 126 へ出力する。コマンドが「データ表示」であれば、コマンド入力部 124 は、「データ表示」を示す信号をデバッグユニット 11 を介してデバッグインターフェース 107 へ送出する。コマンドが「データ書込み」であれば、コマンド入力部 124 は、コマンドに対応する信号を命令・データ入力部 126 へ出力する。コマンドが「終了」であれば、ホスト PC 12 のマイクロプロセッサは処理

を終了する。

【0043】

復号部125は、デバッグユニット11及びデバッグインターフェース107を介して、暗号化回路106から、暗号化回路106により暗号化された暗号化命令を受け取る。また、復号部125は、キーコード入力部123が記憶しているキーコードを読み出す。更に、復号部125は、読み出したキーコードを復号鍵として用い、受け取った暗号化命令に復号アルゴリズム D_1 を施して、復号化命令を生成する。ここで、復号アルゴリズム D_1 は、暗号アルゴリズム E_1 により生成された暗号文を復号するアルゴリズムである。復号部125は、生成した復号化命令を表示部121へ出力する。同様にして、復号部125は、デバッグユニット11及びデバッグインターフェース107を介して、暗号化回路106から、暗号化回路106により暗号化された暗号化データを受け取る。また、復号部125は、キーコード入力部123が記憶しているキーコードを読み出す。更に、復号部125は、読み出したキーコードを復号鍵として用い、受け取った暗号化データに復号アルゴリズム D_1 を施して、復号化データを生成する。ここで、復号アルゴリズム D_1 は、暗号アルゴリズム E_1 により生成された暗号文を復号するアルゴリズムである。復号部125は、生成した復号化データを表示部121へ出力する。

【0044】

不揮発性メモリ105が記憶しているキーコードと、キーコード入力部123が受け付けるキーコードが同じであれば、ホストPC12は、マイクロプロセッサ10から取得した暗号化命令、及び暗号化データを正しく復号することができる。

命令・データ入力部126は、コマンド入力部124から、「命令書込み」を示す信号を受け取ると、命令の入力を受け付けるための画面の生成に用いる画面情報を表示部121へ出力する。命令・データ入力部126は、表示部121に、命令の入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボードを介した命令の入力を受け付ける。命令・データ入力部126は、入力を受け付けた命令をデバッグユニット11を介してデバッグイン

ターフェース 107 へ送出する。命令・データ入力部 126 は、コマンド入力部 124 から、「データ書込み」を示す信号を受け取ると、データの入力を受け付けるための画面の生成に用いる画面情報を表示部 121 へ出力する。命令・データ入力部 126 は、表示部 121 に、データの入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボードを介したデータの入力を受け付ける。命令・データ入力部 126 は、入力を受け付けたデータを、デバッグユニット 11 を介してデバッグインターフェース 107 へ送出する。

【0045】

<動作>

ここでは、図 3 及び図 4 に示すフローチャートを用いて、デバッグシステム 1 の動作について説明する。

ホスト PC 12 のデバッグ部が起動し、キーコード入力部 123 が、ユーザからキーコードの入力を受け付け（ステップ S101）、受け付けたキーコードを記憶する（ステップ S102）。キーコード入力部 123 は、デバッグユニット 11 を介して、マイクロプロセッサ 10 の不揮発性メモリ 105 から、判定フラグを取得し、取得した判定フラグの状態を読み、不揮発性メモリ 105 にキーコードが書き込み済みか否かを判断する（ステップ S103）。キーコードが書き込み済みでない場合（ステップ S104 で NO）、キーコード入力部 123 は、先ほど記憶したキーコードを、デバッグユニット 11 及びデバッグインターフェース 107 を介して不揮発性メモリ 105 に書き込む（ステップ S105）。さらに、キーコード入力部 123 は、キーコードが書き込み済みであることを示す判定フラグを不揮発性メモリ 105 に書き込む（ステップ S106）。

【0046】

次に、ホスト PC 12 のコマンド入力部 124 が、ユーザからコマンドの入力を受け付ける（ステップ S107）。ここで、コマンドの種類は、「命令表示」、「命令書込み」、「データ表示」、「データ書込み」及び「終了」であり、これらの内の何れかがユーザにより選択される。コマンド入力部 124 は、選択されたコマンドを判断する（ステップ S108）。

【0047】

コマンドが「命令表示」であれば（ステップS108で「命令表示」）、コマンド入力部124は、デバッグインターフェース107へ信号を送出し、デバッグインターフェース107は、命令メモリ101に格納されている命令を抽出し（ステップS109）、暗号化回路106に出力する。暗号化回路106は、命令を受け取り、不揮発性メモリ105に保持されているキーコードを用いて、受け取った命令を暗号化する（ステップS110）。暗号化回路106は、暗号化した命令を、デバッグインターフェース107及びデバッグユニット11を介してホストPC12に出力する（ステップS111）。ホストPC12の復号部125は、暗号化された命令を受け取り、ステップS102において記憶したキーコードを用いて受け取った命令を復号する（ステップS112）。復号部125は、復号した命令を表示部121へ出力し、表示部121は、命令を受け取りディスプレイに表示する（ステップS113）。このとき、ステップS101において入力されたキーコードが、不揮発性メモリ105に保持されているキーコードと同じであれば、命令は正しく表示され、キーコードが同じでなければ、命令は正しく表示されない。その後、ステップS107に戻り処理を続ける。

【0048】

コマンドが「命令書込み」であれば（ステップS108で「命令書込み」）、ホストPC12の命令・データ入力部126は、ユーザから命令の入力を受け付ける（ステップS121）。命令・データ入力部126は、受け付けた命令をデバッグユニット11を介してデバッグインターフェース107へ送出し、デバッグインターフェース107は、命令を暗号化回路106へ出力する（ステップS122）。暗号化回路106は、デバッグインターフェース107から命令を受け取り、受け取った命令を命令メモリ101に書き込む（ステップS123）。このとき、暗号化回路106は、命令に暗号化処理を施さず、命令を命令メモリ101に書き込むだけである。その後、ステップS107に戻り処理を続ける。

【0049】

コマンドが「データ表示」であれば（ステップS108で「データ表示」）、コマンド入力部124は、デバッグインターフェース107へ信号を送出し、デバッグインターフェース107は、データメモリ103に格納されているデータ

を抽出し（ステップS131）、暗号化回路106に出力する。暗号化回路106は、データを受け取り、不揮発性メモリ105に保持されているキーコードを用いて、受け取ったデータを暗号化する（ステップS132）。暗号化回路106は、暗号化したデータを、デバッグインターフェース107及びデバッグユニット11を介してホストPC12に出力する（ステップS133）。ホストPC12の復号部125は、暗号化されたデータを受け取り、ステップS102において記憶したキーコードを用いて受け取ったデータを復号する（ステップS134）。復号部125は、復号したデータを表示部121へ出力し、表示部121は、データを受け取りディスプレイに表示する（ステップS135）。このとき、ステップS101において入力されたキーコードが、不揮発性メモリ105に保持されているキーコードと同じであれば、データは正しく表示され、キーコードが同じでなければ、データは正しく表示されない。その後、ステップS107に戻り処理を続ける。

【0050】

コマンドが「データ書込み」であれば（ステップS108で「データ書込み」）、ホストPC12の命令・データ入力部126は、ユーザからデータの入力を受け付ける（ステップS141）。命令・データ入力部126は、受け付けたデータを、デバッグユニット11を介してデバッグインターフェース107へ送出し、デバッグインターフェース107は、データを暗号化回路106へ出力する（ステップS142）。暗号化回路106は、デバッグインターフェース107からデータを受け取り、受け取ったデータをデータメモリ103に書き込む（ステップS143）。このとき、暗号化回路106は、データに暗号化処理を施さず、データをデータメモリ103に書き込むだけである。その後、ステップS107に戻り処理を続ける。

【0051】

コマンドが「終了」であれば（ステップS108で「終了」）、処理を終了する。

2. 第2の実施の形態

本発明に掛かる第2の実施の形態として、デバッグシステム2について図面を

参照して説明する。

【0052】

＜構成＞

ここでは、デバッグシステム 2 の構成について説明する。デバッグシステム 2 は、マイクロプロセッサ 20、デバッグユニット 21 及びホスト PC 22 から構成される。マイクロプロセッサ 20 は、ユーザが開発する IC カードの基板上に搭載されており、デバッグユニット 21 は、ケーブルを介してマイクロプロセッサ 20 及びホスト PC 22 と接続されている。

【0053】

以下では、マイクロプロセッサ 20 及びホスト PC 22 について詳しく説明する。

(マイクロプロセッサ 20)

図 5 は、マイクロプロセッサ 20 の構成を示すブロック図である。同図に示す様に、マイクロプロセッサ 20 は、命令メモリ 201、命令実行ユニット 202、データメモリ 203、データ処理ユニット 204、不揮発性メモリ 205、復号化回路 206 及びデバッグインターフェース 207 から構成される。

【0054】

命令メモリ 201 は、具体的には RAM 及び ROM であって、暗号化命令を記憶している。命令メモリ 201 が記憶している暗号化命令は、予め、ホスト PC 22 のコンパイル部 224 が、命令に暗号アルゴリズム E_2 を施して生成した暗号化命令である。ホスト PC 22 のコンパイル部 224 については後述する。命令メモリ 201 は、バスを介して復号化回路 206 と接続されている。更に、命令メモリ 201 は、バスを介してデバッグインターフェース 207 と接続されており、デバッグユニット 21 を介して接続されたホスト PC 22 上で動作するデバッガの要求を受けて、記憶している暗号化命令をデバッグインターフェース 207 及びデバッグユニット 21 を介してホスト PC 22 へ出力する。また、命令メモリ 201 は、デバッグインターフェース 207 から出力される暗号化命令を受け取り記憶する。

【0055】

命令実行ユニット202は、バスを介して復号化回路206と接続されており、復号化回路206から命令を受け取り、受け取った命令を解釈し、実行する。

データメモリ203は、具体的にはROM又はRAMであってデータを記憶している。データメモリ203は、バスを介してデータ処理ユニット204に接続されており、データ処理ユニット204からの要求を受けて、データ処理ユニット204へデータを出力する。データメモリ203は、データ処理ユニット204が出力する演算結果を受け取り記憶する。更に、データメモリ203は、バスを介してデバッグインターフェース207と接続されており、デバッグユニット21を介して接続されたホストPC22上で動作するデバッグの要求を受けて、記憶しているデータをデバッグインターフェース207へ出力する。また、データメモリ203は、デバッグインターフェース207から出力されるデータを受け取り記憶する。

【0056】

データ処理ユニット204は、バスを介してデータメモリ203と接続されており、データメモリ203からデータを読み出し、読み出したデータに演算処理を施し、演算結果をデータメモリ203に書き込む。

不揮発性メモリ205は、キーコードを記憶する領域と判定フラグを記憶する領域とを備え、キーコードと判定フラグとが書き込まれると、それらを所定の領域に記憶する。キーコードは、復号化回路206による命令の復号化に用いられる復号鍵であって、一度だけ書き込みが可能であり、読み出し及び書き換えが出来ない。判定フラグは、キーコードが不揮発性メモリ205に書き込み済みか否かを判定するために用いるフラグであって、キーコードが不揮発性メモリ205に書き込まれると、判定フラグが不揮発性メモリ205に書き込まれる。また、判定フラグは一度だけ書き込みが可能であり、書き換えが出来ない。

【0057】

復号化回路206は、命令メモリ201に記憶されている暗号化命令を命令実行ユニット202が読み出すときに、暗号化命令を復号化するための回路である。復号化回路206は、不揮発性メモリ205が記憶しているキーコードを復号鍵として用いて命令メモリ201に記憶されている暗号化命令に復号アルゴリズム

ムD₂を施し命令を生成する。ここで、復号アルゴリズムD₂は、暗号アルゴリズムE₂により生成された暗号文を復号するアルゴリズムである。復号化回路206は、生成した命令を命令実行ユニット202へ出力する。

【0058】

デバッグインターフェース207は、デバッグユニット21との接続に用いられるデバッグ端子を含むインターフェースである。デバッグインターフェース207は、デバッグ端子を含み、命令メモリ201とデバッグユニット21、データメモリ203とデバッグユニット21及び不揮発性メモリ205とデバッグユニット21とを接続するインターフェースである。

【0059】

デバッグインターフェース207は、デバッグユニット21を介してホストPC22から「命令表示」を示す信号を受け取ると、命令メモリ201から命令を抽出する。また、「データ表示」を示す信号を受け取ると、データメモリ103からデータを抽出し、抽出したデータをデバッグユニット21へ出力する。また、デバッグインターフェース107は、デバッグユニット21を介してホストPC22から暗号化命令を受け取ると、受け取った暗号化命令を、命令メモリ201へ書き込む。データを受け取ると、受け取ったデータを、データメモリ203へ書き込む。

【0060】

(ホストPC22)

ホストPC22は、マイクロプロセッサ20に対応するデバッガ及びコンパイラが動作するコンピュータシステムであり、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード及びマウスなどから構成されるパーソナルコンピュータである。前記ハードディスクユニットには、デバッガ及びコンパイラを含む各種のコンピュータプログラムが記憶されている。

【0061】

図6は、ホストPC22の構成を示すブロック図である。同図に示す様に、ホストPC22は、表示部221、デバッグ部222、ソースファイル223、コ

ンパイル部 224 及び暗号化オブジェクトファイル 235 を備える。デバッグ部 222 は、前記ハードディスクユニットに記憶されているデバッガが前記マイクロプロセッサにより実行されるとき動作を機能的に示すものであり、デバッグ部 222 は、キーコード入力部 225、コマンド入力部 226、復号部 227、命令・データ入力部 228 及び暗号部 229 を含む。

【0062】

また、コンパイル部 224 は、前記ハードディスクユニットに記憶されているコンパイラが前記マイクロプロセッサにより実行されるとき動作を機能的に示すものであり、コンパイル部 224 は、コンパイル、アセンブル、リンク処理部 231、オブジェクトファイル 232、キーコード入力部 233 及び暗号部 234 を含む。

【0063】

表示部 221 は、ディスプレイユニットを含み、デバッグ部 222 が出力する画面データをディスプレイに表示する。また、表示部 221 は、キーコードの入力を受け付けるための画面がディスプレイに表示されている状態において、キーコード入力部 225 が受け付けた内容を前記画面上に表示する。同様に、表示部 221 は、コマンドの入力を受け付けるための画面がディスプレイに表示されている状態において、コマンド入力部 226 が受け付けた内容を前記画面上に表示する。同様に、表示部 221 は、命令の入力を受け付けるための画面がディスプレイに表示されている状態において、命令・データ入力部 228 が受け付けた内容を前記画面上に表示する。同様に、データの入力を受け付けるための画面がディスプレイに表示されている状態において、命令・データ入力部 228 が受け付けた内容を前記画面上に表示する。

【0064】

キーコード入力部 225 は、キーコードの入力を受け付けるための画面の生成に用いる画面情報を表示部 221 へ出力する。キーコード入力部 225 は、表示部 221 にキーコードの入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボード及びマウスを介したキーコードの入力を受け付け、受け付けたキーコードを記憶する。更に、キーコード入力部 225 は

、デバッグユニット 21 及びマイクロプロセッサ 20 のデバッグインターフェース 207 を介して、不揮発性メモリ 205 から判定フラグを読み、不揮発性メモリ 205 にキーコードが書き込み済みか否か判断する。書き込み済みでない場合、キーコード入力部 225 は、キーコードを、デバッグユニット 21 及びデバッグインターフェース 207 を介して不揮発性メモリ 205 に送出する。キーコード入力部 225 は、デバッグ部 222 の動作が終了すると、記憶したキーコードを破棄する。

【0065】

コマンド入力部 226 は、コマンドの入力を受け付けるための画面の生成に用いる画面情報を表示部 221 へ出力する。コマンド入力部 226 は、表示部 221 にコマンドの入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボード及びマウスを介したコマンドの入力を受け付ける。更に、コマンド入力部 226 は、受け付けたコマンドを判断する。コマンドが「命令表示」であれば、コマンド入力部 226 は、「命令表示」を示す信号を、デバッグユニット 21 を介してデバッグインターフェース 207 へ送出する。コマンドが「命令書込み」であれば、コマンドに対応する信号を命令・データ入力部 228 へ出力する。コマンドが「データ表示」であれば、コマンド入力部 226 は、「データ表示」を示す信号を、デバッグユニット 21 を介してデバッグインターフェース 207 へ送出する。コマンドが「データ書込み」であれば、コマンド入力部 226 は、コマンドに対応する信号を命令・データ入力部 228 へ出力する。コマンドが「終了」であれば、処理を終了する。

【0066】

復号部 227 は、デバッグユニット 21 及びデバッグインターフェース 207 を介して、命令メモリ 201 から暗号化命令を受け取る。また、復号部 227 は、キーコード入力部 225 が記憶しているキーコードを読み出す。更に、復号部 227 は、読み出したキーコードを復号鍵として用い、受け取った暗号化命令に復号アルゴリズム D_2 を施して、復号化命令を生成する。復号部 227 は、生成した復号化命令を表示部 221 へ出力する。

【0067】

不揮発性メモリ 205 が記憶しているキーコードと、キーコード入力部 225 が受け付けるキーコードが同じであれば、ホスト PC 22 は、マイクロプロセッサ 20 から取得した暗号化命令を正しく復号することができる。

命令・データ入力部 228 は、コマンド入力部 226 から、「命令書込み」を示す信号を受け取ると、命令の入力を受け付けるための画面の生成に用いる画面情報を表示部 221 へ出力する。命令・データ入力部 228 は、表示部 221 に、命令の入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボードを介した命令の入力を受け付ける。命令・データ入力部 228 は、入力を受け付けた命令を暗号部 229 へ出力する。命令・データ入力部 228 は、コマンド入力部 226 から、「データ書込み」を示す信号を受け取ると、データの入力を受け付けるための画面の生成に用いる画面情報を表示部 221 へ出力する。命令・データ入力部 228 は、表示部 221 に、データの入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボードを介したデータの入力を受け付ける。命令・データ入力部 228 は、入力を受け付けたデータをデバッグユニット 21 を介してデバッグインターフェース 207 へ送出する。

【0068】

暗号部 229 は、命令・データ入力部 228 から命令を受け取り、キーコード入力部 225 が記憶しているキーコードを読み出す。更に、暗号部 229 は、読み出したキーコードを暗号鍵として用い、受け取った命令に暗号アルゴリズム E₂ を施して、暗号化命令を生成する。暗号部 229 は、生成した暗号化命令をデバッグユニット 21 を介してデバッグインターフェース 207 へ送出する。

【0069】

コンパイル、アセンブル、リンク処理部 231 は、外部記憶装置からソースファイル 223 を読み込み、ソースファイル 223 にコンパイル、アセンブル及びリンク処理を施してオブジェクトファイル 232 を生成する。キーコード入力部 233 は、キーボード及びマウスを介したキーコードの入力を受け付ける。キーコード入力部 233 は、受け付けたキーコードを記憶する。暗号部 234 は、キーコード入力部 233 に記憶されているキーコードを暗号鍵として用いて、オブ

ジェクトファイル 232 に暗号アルゴリズム E₂ を施して暗号化オブジェクトファイル 235 を生成する。コンパイル部 224 は、生成した暗号化オブジェクトファイル 235 を外部記憶装置へ書き込む。

【0070】

<動作>

ここでは、図 3 及び図 7 に示すフローチャートを用いて、デバッグシステム 2 の動作について説明する。

図 3 のステップ S101 からステップ S108 まで、デバッグシステム 2 の動作は、前述したデバッグシステム 1 の動作と同様であるため説明を省略し、図 7 から説明する。

【0071】

コマンドが「命令表示」であれば（ステップ S108 で「命令表示」）、デバッグ部 222 は、コマンドに対応する信号をデバッグユニット 21 を介してデバッグインターフェース 207 へ送出し、デバッグインターフェース 207 は、命令メモリ 201 に格納されている暗号化命令を読み出して、デバッグユニット 21 を介して読み出した暗号化命令を復号部 227 へ渡す（ステップ S201）。復号部 227 は、暗号化命令を受け取り、キーコード入力部 225 が受け付けたキーコードを用いて、受け取った暗号化命令を復号する（ステップ S202）。復号部 227 は、復号した命令を表示部 221 へ出力し、表示部 221 は、命令を受け取りディスプレイに表示する（ステップ S203）。その後、図 3 のステップ S107 に戻り処理を続ける。

【0072】

コマンドが「命令書込み」であれば（ステップ S108 で「命令書込み」）、ホスト PC 22 の命令・データ入力部 228 は、ユーザから命令の入力を受け付ける（ステップ S206）。命令・データ入力部 228 は、受け付けた命令を暗号部 229 へ渡す。暗号部 229 は、キーコード入力部 225 が記憶しているキーコードを読み出し、読み出したキーコードを暗号鍵として用いて、命令を暗号化する（ステップ S207）。暗号部 229 は生成した暗号化命令をデバッグユニット 21 を介してデバッグインターフェース 207 へ送出する（ステップ S2

08)。デバッグインターフェース207は、暗号化命令を受け取り、受け取った暗号化命令を命令メモリ201に格納する（ステップS209）。その後、ステップS107に戻り処理を続ける。

【0073】

コマンドが「データ表示」であれば（ステップS108で「データ表示」）、ホストPC22のデバッグ部222は、コマンドに対応する信号をデバッグユニット21を介してデバッグインターフェース207へ送出し、デバッグインターフェース207は、データメモリ203に格納されているデータを読み出して、デバッグユニット21を介して表示部221に出力する（ステップS221）。表示部221は、データを受け取り、ディスプレイに表示する（ステップS222）。その後、ステップS107に戻り処理を続ける。

【0074】

コマンドが「データ書込み」であれば（ステップS108で「データ書込み」）、ホストPC22の命令・データ入力部228は、ユーザからデータの入力を受け付ける（ステップS231）。命令・データ入力部228は、受け付けたデータを、デバッグユニット21を介してデバッグインターフェース207へ送出手する（ステップS232）。デバッグインターフェース207は、データを受け取り、受け取ったデータをデータメモリ203に格納する（ステップS233）。その後、ステップS107に戻り処理を続ける。

【0075】

コマンドが「終了」であれば（ステップS108で「終了」）、処理を終了する。

<変形例1>

デバッグシステム2の変形例として、デバッグシステム3について説明する。

（構成）

デバッグシステム3は、マイクロプロセッサ30、デバッグユニット31、ホストPC32及び外部メモリ33から構成される。マイクロプロセッサ30と外部メモリ33とは、ユーザが開発するICカードの基板上に搭載されており、外部バスを介して互いに接続されている。また、デバッグユニット31は、ケーブル

ルを介してマイクロプロセッサ 30 及びホスト PC 32 と接続されている。ここで、外部メモリ 33 には、暗号化命令及びデータが記憶されており、前記暗号化命令は、命令にマイクロプロセッサ 30 の不揮発性メモリ 305 に格納されているキーコードと同一の暗号鍵を用い、暗号アルゴリズム E_2 を施して生成したものである。前記暗号化命令は、マイクロプロセッサ 30 により復号され、実行される。

【0076】

デバッグシステム 2 との相違点は、外部メモリ 33 がマイクロプロセッサ 30 に接続されていることである。なお、ホスト PC 32 の構成は図示していない。ホスト PC 32 は、デバッグシステム 2 のホスト PC 22 と同様の構成及び機能を有するため、ここでは説明を省略し、以下ではマイクロプロセッサ 30 について、マイクロプロセッサ 20 との相違点を中心に説明する。

【0077】

図 8 は、マイクロプロセッサ 30 の構成を示すブロック図である。同図に示す様に、マイクロプロセッサ 30 は、命令メモリ 301、命令実行ユニット 302、データメモリ 303、データ処理ユニット 304、不揮発性メモリ 305、復号化回路 306、デバッグインターフェース 307 及びバスコントローラ 308 から構成される。

【0078】

命令メモリ 301、データメモリ 303、不揮発性メモリ 305 及びデバッグインターフェース 307 は、それぞれ、命令メモリ 201、データメモリ 203、不揮発性メモリ 205、デバッグインターフェース 207 と同様の機能を有するため、説明を省略する。

命令実行ユニット 302 は、バスを介して復号化回路 306 と接続されており、復号化回路 306 から命令を受け取り、受け取った命令を解釈し、実行する。ここで、命令実行ユニット 302 が復号化回路 306 から受け取る命令は、命令メモリ 301 に格納されていた暗号化命令を復号化して生成した命令及び外部メモリ 33 に格納されていた暗号化命令と復号化して生成した命令である。

【0079】

データ処理ユニット 304 は、バスを介してデータメモリ 303 と接続されており、データメモリ 303 からデータを読み出し、読み出したデータに演算処理を施し、演算結果をデータメモリ 303 に書き込む。更に、データ処理ユニット 304 は、バス及びバスコントローラ 308 を介して外部メモリ 33 と接続されており、外部メモリ 33 が記憶しているデータを、バスコントローラ 308 を介して読み出し、読み出したデータに演算処理を施し、演算結果を外部メモリ 33 に書き込む。

【0080】

復号化回路 306 は、不揮発性メモリ 305 が記憶しているキーコードを復号鍵として用いて命令メモリ 301 に記憶されている暗号化命令に復号アルゴリズム D_2 を施し復号化命令を生成する。更に、復号化回路 306 は、外部メモリ 33 に記憶されている暗号化命令に復号アルゴリズム D_2 を施し復号化命令を生成する。ここで、復号アルゴリズム D_2 は、暗号アルゴリズム E_2 により生成された暗号文を復号するアルゴリズムである。復号化回路 306 は、生成した復号化命令を命令実行ユニット 202 へ出力する。

【0081】

バスコントローラ 308 は、マイクロプロセッサ 30 の外部に設けられた外部メモリ 33 と命令実行ユニット 302、及び外部メモリ 23 とデータ処理ユニット 304 との間で情報の受け渡しをする。

デバッグシステム 3 の動作は、図 3 及び図 7 に示したデバッグシステム 2 の動作と同様であるため説明を省略する。

【0082】

<変形例 2>

デバッグシステム 2 の変形例として、デバッグシステム 4 について説明する。

(構成)

デバッグシステム 4 は、マイクロプロセッサ 40、デバッグユニット 41 及びホスト PC 42 から構成される。マイクロプロセッサ 40 は、ユーザが開発する IC カードの基板上に搭載されており、デバッグユニット 41 は、ケーブルを介してマイクロプロセッサ 10 及びホスト PC 12 と接続されている。

【0083】

デバッグシステム 2 との相違点は、マイクロプロセッサ 40 は、データに暗号アルゴリズム E_2 を施して生成した暗号化データを内部に保持しており、暗号化データを復号した後にデータ処理を行う。マイクロプロセッサ 40 は、データ処理後の演算結果に暗号アルゴリズム E_2 を施して暗号化データを生成し、生成した暗号化データを記憶する。以下ではマイクロプロセッサ 40 について、マイクロプロセッサ 20 との相違点を中心に説明する。

【0084】

図 9 は、マイクロプロセッサ 40 の構成を示すブロック図である。同図に示す様に、マイクロプロセッサ 30 は、命令メモリ 401、命令実行ユニット 402、データメモリ 403、データ処理ユニット 404、不揮発性メモリ 405、復号化回路 406、デバッグインターフェース 407 及び暗復号化回路 408 から構成される。

【0085】

命令メモリ 401、命令実行ユニット 402 及びデバッグインターフェース 407 は、それぞれ、命令メモリ 201、命令実行ユニット 202 及びデバッグインターフェース 207 と同様の機能を有するため、説明を省略する。

データメモリ 403 は、具体的には ROM 又は RAM であって、暗号化データを保持する。ここで、データメモリ 403 が保持している暗号化データは、データに、不揮発性メモリ 405 が保持しているキーコードと同一のデータを暗号鍵として用い、暗号アルゴリズム E_2 を施して生成したものである。データメモリ 403 は、バスを介して暗復号化回路 408 と接続されており、データ処理ユニット 404 からの要求を受けて、暗号化データを暗復号化回路 408 へ出力する。データメモリ 403 は、暗復号化回路 408 が暗号化した演算結果を受け取り記憶する。更に、データメモリ 403 は、バスを介してデバッグインターフェース 407 と接続されており、デバッグユニット 41 を介して接続されたホスト PC 42 上で動作するデバッガの要求を受けて、記憶している暗号化データをデバッグインターフェース 407 へ出力する。また、データメモリ 403 は、デバッグインターフェース 407 から出力される暗号化データを受け取り記憶する。

【0086】

データ処理ユニット404は、バスを介して暗復号化回路408と接続されており、暗復号化回路408からデータを受け取り、受け取ったデータに演算処理を施し、演算結果を暗復号化回路408に出力する。

復号化回路406は、バスを介して命令メモリ401及び不揮発性メモリ405に接続されており、命令メモリ401から暗号化命令を受け取り、更に、不揮発性メモリ405からキーコードを読み出す。復号化回路406は読み出したキーコードを復号鍵として用い、受け取った暗号化命令に復号アルゴリズム D_2 を施し復号化命令を生成する。ここで、復号アルゴリズム D_2 は、暗号アルゴリズム E_2 により生成された暗号文を復号するアルゴリズムである。復号化回路406は、生成した復号化命令を命令実行ユニット402へ出力する。

【0087】

暗復号化回路408は、暗号化回路と復号化回路とから構成される。暗復号化回路408は、データメモリ403から暗号化データの入力を受け付ける場合、復号化回路を用いてデータを生成し、生成したデータをデータ処理ユニット404へ出力する。暗復号化回路408は、データ処理ユニット404からデータの入力を受け付ける場合、暗号化回路を用いて暗号化データを生成し、生成した暗号化データをデータメモリ403へ出力する。

【0088】

ホストPC42は、マイクロプロセッサ40に対応したデバッガ及びコンパイラが動作するパーソナルコンピュータである。図10に示す様に、ホストPC42は、表示部421、デバッグ部422、ソースファイル423及びコンパイル部424を備える。デバッグ部422は、ホストPC42上で動作するデバッガを機能的に示すもので、キーコード入力部425、コマンド入力部426、復号部427、命令・データ入力部428及び暗号部429を含む。コンパイル部424は、ホストPC42上で動作するコンパイラ、アセンブラ及びリンカを機能的に示すもので、コンパイル、アセンブル、リンク処理部431、オブジェクトファイル432、キーコード入力部433及び暗号部434を含む。ホストPC42は、ホストPC22と同様の機能を有するため、詳細な説明は省略する。

【0089】

(動作)

ここでは、図3及び図11に示すフローチャートを用いて、デバッグシステム4の動作について説明する。

図3のステップS101からステップS108まで、デバッグシステム4の動作は、前述したデバッグシステム1の動作と同様であるため説明を省略し、図11から説明する。

【0090】

コマンドが「命令表示」であれば(ステップS108で「命令表示」)、ホストPC42のデバッグ部422は、コマンドに対応する信号をデバッグユニット41を介してデバッグインターフェース407へ送出し、デバッグインターフェース407は、命令メモリ401に格納されている暗号化命令を読み出して、デバッグユニット41を介して復号部427へ渡す(ステップS401)。復号部427は、デバッグユニット41を介してデバッグインターフェース407から暗号化命令を受け取り、キーコード入力部425が受け付けたキーコードを用いて、受け取った暗号化命令を復号する(ステップS402)。復号部427は、復号した命令を表示部421へ出力し、表示部421は、命令を受け取りディスプレイに表示する(ステップS403)。その後、図3のステップS107に戻り処理を続ける。

【0091】

コマンドが「命令書込み」であれば(ステップS108で「命令書込み」)、ホストPC42の命令・データ入力部228は、ユーザから命令の入力を受け付ける(ステップS411)。命令・データ入力部428は、受け付けた命令を暗号部429へ出力する。暗号部429は、キーコード入力部425が記憶しているキーコードを読み出し、読み出したキーコードを暗号鍵として用いて、命令を暗号化する(ステップS412)。暗号部429は生成した暗号化命令をデバッグユニット41を介してデバッグインターフェース407へ送出する(ステップS413)。デバッグインターフェース407は、暗号化命令を受け取り、受け取った暗号化命令を命令メモリ401に格納する(ステップS414)。その後

、ステップS107に戻り処理を続ける。

【0092】

コマンドが「データ表示」であれば（ステップS108で「データ表示」）、ホストPC42のデバッグ部422は、コマンドに対応する信号をデバッグユニット41を介してデバッグインターフェース407へ送出し、デバッグインターフェース407は、データメモリ403に格納されている暗号化データを読み出し、デバッグユニット41を介して復号部427に渡す（ステップS421）。復号部427は、デバッグユニット41を介してデバッグインターフェース407から暗号化データを受け取り、キーコード入力部425が受け付けたキーコードを用いて、受け取った暗号化データを復号する（ステップS422）。復号部427は、復号したデータを表示部421へ出力し、表示部421は、データを受け取りディスプレイに表示する（ステップS423）。その後、図3のステップS107に戻り処理を続ける。

【0093】

コマンドが「データ書込み」であれば（ステップS108で「データ書込み」）、ホストPC42の命令・データ入力部428は、ユーザからデータの入力を受け付ける（ステップS431）。命令・データ入力部428は、受け付けたデータを暗号部429へ渡す。暗号部429は、キーコード入力部425が記憶しているキーコードを読み出し、読み出したキーコードを暗号鍵として用いて、データを暗号化する（ステップS432）。暗号部429は生成した暗号化データをデバッグユニット41を介してデバッグインターフェース407へ送出する（ステップS433）。デバッグインターフェース407は、暗号化データを受け取り、受け取った暗号化データをデータメモリ403に格納する（ステップS434）。その後、ステップS107に戻り処理を続ける。

【0094】

コマンドが「終了」であれば（ステップS108で「終了」）、処理を終了する。

＜変形例3＞

デバッグシステム2の変形例として、デバッグシステム5について説明する。

(構成)

デバッグシステム 5 は、図 12 に示す様に、マイクロプロセッサ 50、メモリリードライト装置 51 及びホスト PC 52 から構成される。マイクロプロセッサ 50 は、ユーザが開発する IC カードの基板上に搭載されている。メモリリードライト装置 51 は、マイクロプロセッサ 50 のメモリのプログラム及びデータの読み出し、及びマイクロプロセッサ 50 のメモリにプログラム及びデータの書き込みを行う装置であって、マイクロプロセッサ 50 及びホスト PC 52 と、それぞれケーブルを介して接続されている。

【0095】

マイクロプロセッサ 50 は、命令メモリ 501、命令実行ユニット 502、データメモリ 503、データ処理ユニット 504、不揮発性メモリ 505、復号化回路 506 及びデバッグインターフェース 507 から構成される。マイクロプロセッサ 50 は、図 5 に示したマイクロプロセッサ 20 と同様の構成を有するため、マイクロプロセッサ 50 の構成を示すブロック図は示していない。マイクロプロセッサ 50 の各構成要素は、それぞれ、マイクロプロセッサ 20 の命令メモリ 201、命令実行ユニット 202、データメモリ 203、データ処理ユニット 204、不揮発性メモリ 205、復号化回路 206 及びデバッグインターフェース 207 を同様の機能を有するため、ここでは説明を省略する。

【0096】

ホスト PC 52 は、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード及びマウスなどから構成されるパーソナルコンピュータである。前記ハードディスクユニットには、メモリリードライト装置制御プログラムを含む各種のコンピュータプログラムが記憶されている。

【0097】

図 11 は、ホスト PC 52 の機能を示す機能ブロック図である。同図に示す様に、ホスト PC 52 は、表示部 521、メモリリードライト装置制御部 522、ソースファイル 523 及びコンパイル部 524 を備える。メモリリードライト装置制御部 522 は、更に、キーコード入力部 525、メモリ操作コマンド入力部

526、復号部527及び暗号部528を含む。

【0098】

表示部521は、ディスプレイユニットを含み、メモリリードライト装置制御部522が出力する画面データをディスプレイに表示する。また、表示部521は、キーコードの入力を受け付けるための画面がディスプレイに表示されている状態において、キーコード入力部525が受け付けた内容を前記画面上に表示する。同様に、表示部521は、コマンドの入力を受け付けるための画面がディスプレイに表示されている状態において、メモリ操作コマンド入力部526が受け付けた内容を前記画面上に表示する。

【0099】

キーコード入力部525は、具体的にはキーボード及びマウス等を含み、キーコードの入力を受け付けるための画面の生成に用いる画面情報を表示部521へ出力する。キーコード入力部525は、表示部521にキーコードの入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボード及びマウスを介したキーコードの入力を受け付ける。キーコード入力部525は、受け付けたキーコードを記憶する。更に、キーコード入力部525は、受け付けたキーコードを、メモリリードライト装置51を介してデバッグインターフェース507へ送出する。キーコード入力部525は、メモリリードライト装置制御部522の動作が終了すると、記憶しているキーコードを破棄する。

【0100】

メモリ操作コマンド入力部526は、具体的にはキーボード及びマウス等を含み、コマンドの入力を受け付けるための画面の生成に用いる画面情報を表示部521へ出力する。メモリ操作コマンド入力部526は、表示部521にコマンドの入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボード及びマウスを介したコマンドの入力を受け付ける。更に、メモリ操作コマンド入力部526は、受け付けたコマンドを判断する。

【0101】

コマンドが「メモリ読出し」であれば、メモリ操作コマンド入力部526は、コマンドに対応する信号を、メモリリードライト装置51を介してデバッグイン

ターフェース 507 へ送出する。コマンドが「メモリ書込み」であれば、メモリ操作コマンド入力部 526 は、コンパイル部 524 にファイルを指定する信号を出力する。コマンドが「終了」であれば、マイクロプロセッサは処理を終了する。

【0102】

復号部 527 は、メモリリードライト装置 51 を介してマイクロプロセッサ 50 から暗号化命令を受け取り、キーコード入力部 525 が記憶しているキーコードを読み出す。更に、復号部 527 は、読み出したキーコードを復号鍵として用い、受け取った暗号化命令に復号アルゴリズム D_2 を施して、復号化命令を生成する。復号部 527 は、生成した復号化命令を表示部 521 へ出力する。

【0103】

不揮発性メモリ 505 が記憶しているキーコードと、キーコード入力部 525 が受け付けるキーコードが同じであれば、ホスト PC 52 は、マイクロプロセッサ 50 から取得した暗号化命令を正しく復号することができる。

暗号部 528 は、外部記憶装置からオブジェクトファイル 532 を読み出す。また、キーコード入力部 525 が記憶しているキーコードを読み出す。暗号部 528 は、読み出したキーコードを暗号鍵として用い、読み出したオブジェクトファイルに暗号アルゴリズム E_2 を施して、暗号化ファイルを生成する。暗号部 229 は、生成した暗号化ファイルをメモリリードライト装置 51 を介してマイクロプロセッサ 50 へ送出する。

【0104】

コンパイル部 524 は、ホスト PC 52 上で動作するコンパイラ、アセンブラ及びリンカを機能的に示すもので、コンパイル部 524 は、メモリ操作コマンド入力部 526 から指示を受け取り、受け取った指示に対応するファイルを、外部記憶装置に記憶されているソースファイル 523 から読み込む。コンパイル部 524 は、読み込んだソースファイルに、コンパイル、アセンブル及びリンク処理を施してオブジェクトファイル 532 生成し、生成したオブジェクトファイル 532 を外部記憶装置に書く。

【0105】

(動作)

ここでは、図3及び図13に示すフローチャートを用いて、デバッグシステム5の動作について説明する。図3のステップS101からステップS108まで、デバッグシステム5の動作は、前述したデバッグシステム1の動作と同様であるため説明を省略し、図13から説明する。

【0106】

コマンドが「メモリ書込み」であれば（ステップS108で「メモリ書込み」）、ホストPC52のメモリ操作コマンド入力部526は、書き込むデータファイルの指定を受け付ける（ステップS501）。メモリ操作コマンド入力部526は、指定されたオブジェクトファイルを、外部記憶装置から読み込み（ステップS502）、暗号部528に渡す。暗号部528は、オブジェクトファイルを受け取り、受け取ったオブジェクトファイルに、キーコード入力部525が記憶しているキーコードを暗号鍵として用い、暗号アルゴリズムE₂を施し暗号化する（ステップS503）。暗号部528は、メモリリードライト装置51を介してマイクロプロセッサ50に暗号化データを出力し（ステップS504）、マイクロプロセッサ50の命令メモリ501及びデータメモリ503に書き込む（ステップS505）。

【0107】

コマンドが「メモリ読出し」であれば（ステップS108で「メモリ読出し」）、ホストPC52のメモリリードライト装置制御部522は、コマンドに対応する信号を、メモリリードライト装置51を介してデバッグインターフェース507へ送出する。デバッグインターフェース507は、命令メモリ501及びデータメモリ503を読み出し、暗号化命令及び暗号化データを、メモリリードライト装置51を介して復号部527へ出力する（ステップS511）。復号部527は、暗号化命令及び暗号化データを受け取り、キーコード入力部425が受け付けたキーコードを用いて、受け取った暗号化命令及び暗号化データを復号する（ステップS512）。復号部527は、復号した命令及びデータを表示部521へ出力し、表示部521は、命令及びデータを受け取りディスプレイに表示する（ステップS513）。その後、図3のステップS107に戻り処理を続け

る。

【0108】

コマンドが「終了」であれば、マイクロプロセッサは処理を終了する。

3. 第3の実施の形態

本発明に係る第3の実施の形態として、デバッグシステム6について図面を参照して説明する。

<構成>

ここでは、デバッグシステム6の構成について説明する。デバッグシステム6は、マイクロプロセッサ60、デバッグユニット61、ホストPC62及び外部メモリ63から構成される。マイクロプロセッサ60と外部メモリ63とは、ユーザが開発するICカードの基板上に搭載されており、外部バスを介して互いに接続されている。デバッグユニット61は、ケーブルを介してマイクロプロセッサ60及びホストPC62と接続されている。外部メモリ63は、 $n-1$ 個のメモリブロックに分割されており、各メモリブロックには、命令及びデータから成るコンピュータプログラムが記憶されている。各コンピュータプログラムは、マイクロプロセッサ60により実行される。

デバッグシステム6では、複数の開発者が、それぞれの開発段階において固有のキーコードを用いてマイクロプロセッサ60のデバッグを行うことが可能である。以下では、マイクロプロセッサ60及びホストPC62について詳しく説明する。

【0109】

(マイクロプロセッサ60)

図14は、マイクロプロセッサ60の構成を示すブロック図である。同図に示す様に、マイクロプロセッサ60は、命令メモリ601、命令実行ユニット602、データメモリ603、データ処理ユニット604、不揮発性メモリ605、復号化回路606、デバッグインターフェース607、バスコントローラ608及びアドレスデコーダ609から構成される。

【0110】

命令メモリ601は、具体的にはRAM及びROMであって、暗号化命令を記

憶している。命令メモリ 601 が記憶している暗号化命令は、予め、命令に暗号アルゴリズム E_3 を施して生成したものである。暗号アルゴリズム E_3 の一例は DES である。命令メモリ 601 は、バスを介して復号化回路 606 と接続されており、命令実行ユニット 602 の要求に従い、暗号化命令を復号化回路 606 へ出力する。更に、命令メモリ 601 は、バスを介してデバッグインターフェース 607 と接続されており、デバッグユニット 61 を介して接続されたホスト PC 62 上で動作するデバッグの要求を受けて、記憶している暗号化命令をデバッグインターフェース 607 及びデバッグユニット 61 を介してホスト PC 62 へ出力する。また、命令メモリ 601 は、デバッグインターフェース 607 から出力される暗号化命令を受け取り記憶する。

【0111】

命令実行ユニット 602 は、バスを介して復号化回路 606 と接続されており、復号化回路 606 から命令を受け取り、受け取った命令を解釈し、実行する。更に、命令実行ユニット 602 は、バスコントローラ 608 及び外部バスを介して外部メモリ 63 と接続されており、外部メモリ 63 の各メモリブロックが記憶している命令を、バスコントローラ 608 を介して読み出し、解釈し、実行する。

【0112】

データメモリ 603 は、具体的には ROM 又は RAM であってデータを記憶している。データメモリ 603 は、バスを介してデータ処理ユニット 604 に接続されており、データ処理ユニット 604 からの要求を受けて、データ処理ユニット 604 へデータを出力する。データメモリ 603 は、データ処理ユニット 604 が出力する演算結果を受け取り記憶する。更に、データメモリ 603 は、バスを介してデバッグインターフェース 607 と接続されており、デバッグユニット 61 を介して接続されたホスト PC 62 上で動作するデバッグの要求を受けて、記憶しているデータをデバッグインターフェース 607 及びデバッグユニット 61 を介してホスト PC 62 へ出力する。また、データメモリ 603 は、デバッグインターフェース 607 から出力されるデータを受け取り記憶する。

【0113】

データ処理ユニット 604 は、バスを介してデータメモリ 603 と接続されており、データメモリ 603 からデータを読み出し、読み出したデータに演算処理を施し、演算結果をデータメモリ 603 に書き込む。更に、データ処理ユニット 604 は、外部バス及びバスコントローラ 608 を介して外部メモリ 63 と接続されており、外部メモリ 63 の各メモリブロックが記憶しているデータを、バスコントローラ 608 を介して読み出し、読み出したデータに演算処理を施し、演算結果を各メモリブロックに書き込む。

【0114】

不揮発性メモリ 605 は、「キーコード 1」から「キーコード n」までの n 個のキーコードと、「判定フラグ F 1」から「判定フラグ F n」までの n 個の判定フラグとを記憶する領域を備え、各キーコードと各判定フラグとが書き込まれると、それらを所定の領域に記憶する。

「キーコード 1」は、命令メモリ 601 が記憶している暗号化命令を復号するときに用いられる復号鍵である。「判定フラグ F 1」は、「キーコード 1」が不揮発性メモリ 605 に書き込み済みか否かを判定するために用いるフラグであって、「キーコード 1」が不揮発性メモリ 605 に書き込まれると、「判定フラグ F 1」が不揮発性メモリ 605 に書き込まれる。「キーコード 2」は、外部メモリ 63 のメモリブロック 1 に記憶されている暗号化命令を復号するときに用いられる復号鍵である。「判定フラグ F 2」は、「キーコード 2」が不揮発性メモリ 605 に書き込み済みか否かを判定するために用いるフラグである。同様に、「キーコード n」は、外部メモリ 63 のメモリブロック n-1 に記憶されている暗号化命令を復号するときに用いられる復号鍵である。「判定フラグ F N」は、「キーコード N」が不揮発性メモリ 605 に書き込み済みか否かを判定するために用いるフラグである。

【0115】

なお、「キーコード 1」から「キーコード n」は、それぞれ、一度だけ書き込みが可能であり、読み出し及び書き換えが出来ない。また、「判定フラグ F 1」から「判定フラグ F n」は、それぞれ、一度だけ書き込みが可能であり、書き換えが出来ない。

復号化回路 606 は、命令メモリ 601 及び外部メモリ 63 の各メモリブロックに記憶されている暗号化命令を命令実行ユニット 602 が実行するために、復号化する回路である。復号化回路 606 は、命令メモリ 601 及び外部メモリ 63 の各メモリブロックから暗号化命令を受け取る。復号化回路 606 は、対応するキーコードを不揮発性メモリから取得し、取得したキーコードを復号鍵として用いて暗号化命令に復号アルゴリズム D_3 を施し復号化命令を生成する。ここで、復号アルゴリズム D_3 は、暗号アルゴリズム E_3 により生成された暗号文を復号するアルゴリズムである。復号化回路 606 は、生成した復号化命令を命令実行ユニット 602 へ出力する。

【0116】

デバッグインターフェース 607 は、命令メモリ 601 とデバッグユニット 61、データメモリ 603 とデバッグユニット 61 及び不揮発性メモリ 605 とデバッグユニット 61 との接続に用いられるインターフェースであって、不揮発性メモリ 605 を保護する。デバッグインターフェース 607 は、第 2 の実施の形態におけるデバッグインターフェース 207 と同様の機能を有するため、詳細な説明は省略する。

【0117】

バスコントローラ 608 は、マイクロプロセッサ 60 の外部に設けられた外部メモリ 63 と命令実行ユニット 602、及び外部メモリ 63 とデータ処理ユニット 604 との間で、外部バスを介して情報の受け渡しをする。

アドレスデコーダ 609 は、バスを介して命令メモリ 601 及び外部メモリ 63 に接続されており、命令実行ユニット 602 から出力されるアドレスに対応して、命令メモリ 601、外部メモリ 63 の各メモリブロックを選択すると共に、選択されたメモリブロックに対応するキーコードを不揮発性メモリ 605 から読み出し、復号化回路 606 に出力する。

【0118】

(ホスト PC 62)

ホスト PC 62 は、マイクロプロセッサ 60 に対応したデバッガが動作するパーソナルコンピュータであり、マイクロプロセッサ 60 の命令メモリ 601 を観

察可能な開発者が有するPCである。ホストPC62は、図15に示す様に、表示部621とデバッグ部622とを備え、デバッグ部622は、キーコード入力部625、コマンド入力部626、復号部627、命令・データ入力部628及び暗号部629を含む。各部の機能はホストPC22の表示部221及びデバッグ部622と同様であるため、詳細な説明を省略する。

【0119】

<動作>

ここでは、図16に示すフローチャートを用いてデバッグシステム6の動作について説明する。

ホストPC62のデバッグ部622が起動し、キーコード入力部625が、ユーザの操作によりキーコード番号Mの入力を受け付ける（ステップS600）。ここで、Mは、 $1 \leq M \leq n$ を満たす整数である。

【0120】

続いて、キーコード入力部625は、キーコードNの入力を受け付け（ステップS601）、受け付けたキーコードNを記憶する（ステップS602）。キーコード入力部625は、受け付けたキーコードNを、デバッグユニット61を介してデバッグインターフェース607へ送出する。デバッグインターフェース607は、キーコードNを受け取ると、不揮発性メモリ605の「判定フラグFN」の状態を読み、不揮発性メモリ605内のキーコードNが書き込まれるべき領域に、キーコードNが書き込み済みか否かを判断する（ステップS603）。前記領域にキーコードNが書き込み済みでない場合（ステップS604でNO）、デバッグインターフェース607は、受け取ったキーコードNを不揮発性メモリ605に書き込む（ステップS605）。さらに、デバッグインターフェース607は、キーコードNが書き込み済みであることを示す「判定フラグFN」を不揮発性メモリ605に書き込む（ステップS606）。

【0121】

次に、コマンド入力部626が、ユーザからコマンドの入力を受け付ける（ステップS607）。ここで、コマンドの種類は、「命令表示」、「命令書込み」、「データ表示」、「データ書込み」及び「終了」であり、これらの内の何れか

一つがユーザにより選択される。コマンド入力部 626 は、選択されたコマンドを判断する（ステップ S608）。以下、図 7 に示したフローチャートに続く。

【0122】

4、第 4 の実施の形態

本発明に係る第 4 の実施の形態として、デバッグシステム 7 について、図面を参照して説明する。

<構成>

ここでは、デバッグシステム 7 の構成について説明する。デバッグシステム 7 は、マイクロプロセッサ 70、デバッグユニット 71 及びホスト PC 72 から構成される。マイクロプロセッサ 70 は、ユーザが開発する IC カードの基板上に搭載されており、デバッグユニット 71 は、ケーブルを介してマイクロプロセッサ 70 及びホスト PC 72 と接続されている。以下では、マイクロプロセッサ 70 及びホスト PC 72 について詳細に説明する。

【0123】

(マイクロプロセッサ 70)

図 17 は、マイクロプロセッサ 70 の構成を示すブロック図である。同図に示す様に、マイクロプロセッサ 70 は、命令メモリ 701、命令実行ユニット 702、データメモリ 703、データ処理ユニット 704、不揮発性メモリ 705、暗号化回路 706、デバッグインターフェース 707、セキュリティヒューズ 708 及びバッファ 709 から構成される。

【0124】

命令メモリ 701 は、具体的には RAM 及び ROM であって命令を記憶している。命令メモリ 701 は、バスを介して命令実行ユニット 702 と接続されている。更に、命令メモリ 701 は、バスを介して暗号化回路 706 と接続されており、デバッグユニット 71 を介して接続されたホスト PC 72 上で動作するデバッグの要求を受けて、記憶している命令を暗号化回路 706 へ出力する。また、命令メモリ 701 は、暗号化回路 706 から出力される命令を受け取り記憶する。

【0125】

命令実行ユニット 702 は、バスを介して命令メモリ 701 と接続されており、命令メモリ 701 が記憶している命令を読み出し、解釈し、実行する。

データメモリ 703 は、具体的には ROM 又は RAM であってデータを記憶している。データメモリ 703 は、バスを介してデータ処理ユニット 704 に接続されており、データ処理ユニット 704 からの要求を受けて、データ処理ユニット 704 へデータを出力する。データメモリ 703 は、データ処理ユニット 704 が出力する演算結果を受け取り記憶する。更に、データメモリ 703 は、バスを介して暗号化回路 706 と接続されており、デバッグユニット 71 を介して接続されたホスト PC 72 上で動作するデバッガの要求を受けて、記憶しているデータを暗号化回路 706 へ出力する。また、データメモリ 703 は、暗号化回路 706 から出力されるデータを受け取り記憶する。

【0126】

データ処理ユニット 704 は、バスを介してデータメモリ 703 と接続されており、データメモリ 703 からデータを読み出し、読み出したデータに演算処理を施し、演算結果をデータメモリ 703 に書き込む。

不揮発性メモリ 705 は、キーコードを記憶する領域と判定フラグを記憶する領域とを備え、キーコードと判定フラグとが書き込まれると、それらを所定の領域に記憶する。キーコードは、暗号化回路 706 による命令の暗号化及びデータの暗号化に用いられる暗号鍵であって、一度だけ書き込みが可能であり、読み出し及び書き換えが出来ない。判定フラグは、キーコードが不揮発性メモリ 705 に書き込み済みか否かを判定するために用いるフラグであって、キーコードが不揮発性メモリ 705 に書き込まれると、判定フラグが不揮発性メモリ 705 に書き込まれる。また、判定フラグは一度だけ書き込みが可能であり、書き換えが出来ない。

【0127】

暗号化回路 706 は、ホスト PC 72 からの要求を受けて、命令メモリ 701 に記憶されている命令をデバッグインターフェース 707 が読み出すとき、また、データメモリ 703 に記憶されているデータをデバッグインターフェース 707 が読み出すときに命令及びデータを暗号化するための回路である。暗号化回路

706は、不揮発性メモリ705が記憶しているキーコードを暗号鍵として用いて命令メモリ701に記憶されている命令及びデータメモリ703に記憶されているデータに、暗号アルゴリズム E_4 を施し暗号化命令及び暗号化データを生成する。ここで暗号アルゴリズム E_4 は、例としてDESである。暗号化回路706は、生成した暗号化命令及び暗号化データをデバッグインターフェース707へ出力する。

【0128】

デバッグインターフェース707は、暗号化回路706とバッファ709、及び不揮発性メモリ705とバッファ709との接続に用いられ、暗号化回路706及び不揮発性メモリ705を保護する。デバッグインターフェース707は、第1の実施の形態におけるデバッグインターフェース107とほぼ同様の機能を有するが、デバッグインターフェース107と異なり、暗号化回路706から暗号化命令及び暗号化データを受け取ると、受け取った暗号化命令及び暗号化データをバッファ709に出力する。

【0129】

セキュリティヒューズ708は、「0」又は「1」のフラグであって、「0」は、セキュリティヒューズが切断された状態であり、バッファ709の出力を抑制することを示す。「1」は、バッファ709は通常通り出力することを示す。セキュリティヒューズ708は、初期状態ではフラグは、「1」に設定されている。セキュリティヒューズ708は、デバッグユニット71を介してホストPC72の比較部728から指示を受けてフラグを「1」から「0」へ書き換える。なお、「1」から「0」に書き換えられたフラグを再度「1」に書き換えることは出来ない。

【0130】

バッファ709は、バスを介してデバッグインターフェース707及びセキュリティヒューズ708と接続されている。バッファ709は、セキュリティヒューズ708の状態を読み出す。読み出したセキュリティヒューズ708の状態が「0」の場合、バッファ709は、デバッグインターフェース707から暗号化命令と暗号化データとを受け取ると、デバッグユニット71との接続を切断する

。セキュリティヒューズ708の状態が「1」の場合、バッファ709は通常通りにデバッグユニット71と接続され、デバッグインターフェース707から受け取る暗号化命令と暗号化データとをデバッグユニット71へ出力する。

【0131】

(ホストPC72)

ホストPC72は、マイクロプロセッサ70に対応したデバッガが動作するパーソナルコンピュータである。

図18は、ホストPC72の構成を示すブロック図である。同図に示す様に、ホストPC72は、表示部721、デバッグ部722及びカウンタ741を備える。デバッグ部722は、ホストPC72上で動作するデバッガを機能的に示すもので、キーコード入力部723、コマンド入力部724、復号部725、命令・データ入力部726、指定回数記憶部727及び比較部728を含む。

【0132】

表示部721は、ディスプレイユニットを含み、各種の画面をディスプレイに表示する。表示部721は、デバッグシステム1の表示部121と同様の機能を有するため、詳細な説明を省略する。

カウンタ741は、外部記憶装置に記憶されており、キーコード入力部723が、前回受け付けたキーコードと異なるキーコードを何回受け付けたのかをカウントする。カウンタ741は、キーコード入力部723からの指示を受け、記憶している数値に1を加算する。

【0133】

キーコード入力部723は、キーボード及びマウス等を含む。キーコード入力部723は、内部に記憶領域を備え、キーコード入力部723が前回入力を受け付けたキーコード（以下「前回キーコード」と呼称する）を前記記憶領域に記憶している。キーコード入力部723は、表示部721にキーコードの入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボード及びマウスを介したキーコードの入力を受け付ける。キーコード入力部723は、キーコードの入力を受け付けると、受け付けた当該キーコードと前回キーコードとが一致するか否かを判定する。不一致の場合、キーコード入力部723

は、カウンタ 741 に対して、記憶している数値に 1 を加算する信号を出力し、前記領域に記憶されている前回キーコードに当該キーコードを上書きする。

【0134】

また、キーコード入力部 723 は、当該キーコードを、デバッグユニット 71、バッファ 709 及びデバッグインターフェース 707 を介して不揮発性メモリ 705 に送出する。

コマンド入力部 724 は、第 1 の実施の形態におけるコマンド入力部 124 と同様の機能を有するため、ここでは説明を省略する。

【0135】

復号部 725 は、デバッグユニット 71 及びバッファ 709 を介して、デバッグインターフェース 707 から暗号化命令を受け取る。また、復号部 725 は、キーコード入力部 723 が記憶しているキーコードを読み出す。更に、復号部 725 は、読み出したキーコードを復号鍵として用い、受け取った暗号化命令に復号アルゴリズム D_4 を施して、復号化命令を生成する。ここで、復号アルゴリズム D_4 は、暗号アルゴリズム E_4 により生成された暗号文を復号するアルゴリズムである。復号部 725 は、生成した復号化命令を表示部 721 へ出力する。同様にして、復号部 725 は、暗号化データを取得し、取得した暗号化データにキーコードを復号鍵として用い、取得した暗号化データに復号アルゴリズム D_4 を施して、復号化データを生成する。復号部 725 は、生成した復号化データを表示部 721 へ出力する。

【0136】

命令・データ入力部 726 は、第 1 の実施の形態における命令・データ入力部 126 と同様の機能を有するため、ここでは説明を省略する。

指定回数記憶部 727 は、指定回数を示す数値を保持する。ここで、指定回数とはキーコード入力部 723 がユーザから受け付けるキーコードが前回キーコードと異なる場合において、異なるキーコードを受け付けた回数が当該指定回数を越えた場合にデバッグを停止するために用いる数値である。

【0137】

比較部 728 は、カウンタ 741 が記憶している数値と指定回数記憶部 727

が記憶している数値とを読み、比較する。カウンタ 741 が記憶している数値が、指定回数記憶部 727 が記憶している数値よりも大きい場合、比較部 728 は、デバッグユニット 71 を介してフラグを「0」に書き換える信号をセキュリティヒューズ 708 へ出力する。

【0138】

<動作>

ここでは、図 19 及び図 20 に示すフローチャートを用いて、デバッグシステム 7 の動作について説明する。

ホスト PC 72 のキーコード入力部 723 は、判定フラグの状態を読み（ステップ S701）、不揮発性メモリ 705 にキーコードが書き込み済みか否か判断する。不揮発性メモリ 705 にキーコードが書き込み済みの場合（ステップ S702 で YES）、キーコード入力部 723 は、ユーザからキーコードの入力を受け付ける（ステップ S703）。キーコード入力部 723 は、受け付けたキーコードを記憶する（ステップ S704）。

【0139】

キーコード入力部 723 は、内部に記憶している前回キーコードを読み（ステップ S705）、受け付けたキーコードが前回キーコードに一致するか否か判断する。一致しない場合（ステップ S706 で NO）、カウンタ 741 は、キーコード入力部 723 からの信号を受けて、記憶している数値に 1 を加算する（ステップ S707）。次に、比較部 728 は、カウンタ 741 が記憶している数値と指定回数記憶部 727 が記憶している指定回数とを読み出し、比較する（ステップ S708）。カウンタ 741 が記憶している値が、指定回数よりも大きい場合（ステップ S709 で YES）、比較部 728 は、セキュリティヒューズ 708 のフラグを「0」に書き換える指示を出力し、セキュリティヒューズを切断する（ステップ S710）。カウンタ 741 が記憶している値が、指定回数よりも小さい場合（ステップ S709 で NO）、ステップ S703 に戻り処理を続ける。

【0140】

キーコード入力部 723 は、判定フラグを読み出した結果、不揮発性メモリ 705 にキーコードが書き込まれていない場合（ステップ S702 で NO）、ユー

ザからキーコードの入力を受け付ける（ステップS721）。キーコード入力部723は、受け付けたキーコードを記憶すると共に（ステップS722）、デバッグユニット71、バッファ709及びデバッグインターフェース707を介して不揮発性メモリ705に受け付けたキーコードを書き込む（ステップS723）。次に、キーコード入力部723は、デバッグユニット71、バッファ709及びデバッグインターフェース707を介して不揮発性メモリに、キーコードが書き込み済みであることを示す判定フラグを書き込む（ステップS724）。

【0141】

次に、ホストPC72のコマンド入力部724が、ユーザからコマンドの入力を受け付ける（ステップS725）。ここで、コマンドの種類は、「命令表示」、「命令書込み」、「データ表示」、「データ書込み」及び「終了」であり、これらの内の何れかがユーザにより選択される。コマンド入力部724は、選択されたコマンドを判断する（ステップS726）。以下、図4に示したフローチャートに続く。

【0142】

受け付けたキーコードが前回キーコードに一致する場合は（ステップS706でYES）、ステップS725に続く。

5. 第5の実施の形態

本発明に係る第5の実施の形態として、デバッグシステム8について、図面を参照して説明する。デバッグシステム8は、デバッグシステム7におけるキーコード比較処理を、ホストPC側が行うのではなく、マイクロプロセッサ側が行うことが特徴である。

【0143】

<構成>

ここでは、デバッグシステム8の構成について説明する。デバッグシステム8は、マイクロプロセッサ80、デバッグユニット81及びホストPC82から構成される。マイクロプロセッサ80は、ユーザが開発するICカードの基板上に搭載されており、デバッグユニット81は、ケーブルを介してマイクロプロセッサ80及びホストPC82と接続されている。

【0144】

ホストPC82は、表示部821及びデバッグ部822から構成され、デバッグ部822は、更に、キーコード入力部823、コマンド入力部824、復号部825及び命令・データ入力部826から構成される。なお、ホストPC82の構成は図示していない。ホストPC82の各構成要素は、第1の実施の形態におけるホストPC12の各構成要素と同様の機能を有するため説明を省略する。

【0145】

以下では、マイクロプロセッサ80の構成について説明する。

(マイクロプロセッサ80)

図21は、マイクロプロセッサ80の構成を示すブロック図である。同図に示す様に、マイクロプロセッサ80は、命令メモリ801、命令実行ユニット802、データメモリ803、データ処理ユニット804、不揮発性メモリ805、暗号化回路806、デバッグインターフェース807、前回キーコード記憶部808、指定回数記憶部809、カウンタ810、比較部811、セキュリティヒューズ812及びバッファ813から構成される。

【0146】

命令メモリ801、命令実行ユニット802、データメモリ803、データ処理ユニット804、不揮発性メモリ805、暗号化回路806及びバッファ813は、それぞれ、第4の実施の形態における命令メモリ701、命令実行ユニット702、データメモリ703、データ処理ユニット704、不揮発性メモリ705、暗号化回路706及びバッファ709と同様の機能を有するため、ここでは説明を省略する。

【0147】

デバッグインターフェース807は、暗号化回路806とバッファ813、不揮発性メモリ805とバッファ813、及び前回キーコード記憶部808とカウンタ810の接続に用いられる。

前回キーコード記憶部808は、キーコードを記憶する領域を備え、前回、バッファ813から受け取ったキーコード（以下、前回キーコードと呼称する）を記憶する。前回キーコード記憶部808は、ホストPC82のキーコード入力部

823が受け付けたキーコードを、デバッグユニット81及びバッファ813を介してデバッグインターフェース807から受け取り、受け取った当該キーコードと記憶している前回キーコードとを比較する。前回キーコード記憶部808は、両者が異なる場合に、カウンタ810に対して記憶している数値に1を加算する信号を出力し、更に、比較部811に対してカウンタ810が記憶している数値と指定回数記憶部809が記憶している数値とを比較する信号を出力する。

【0148】

指定回数記憶部809は、予め、一度だけ書き込みが可能な指定回数を示す数値を記憶している。指定回数とは、ホストPC82がユーザから受け付けるキーコードが前回受け付けたキーコードと異なる場合において、異なるキーコードを受け付けた回数が当該指定回数を越えた場合にセキュリティヒューズ812を切断し、デバッグを停止するために用いる数値である。

【0149】

カウンタ810は、ホストPC82が、前回キーコード記憶部808が記憶しているキーコードと異なるキーコードを受け付けた回数をカウントする。カウンタ810は、前回キーコード記憶部808からの指示を受け、記憶している数値に1を加算する。

比較部811は、前回キーコード記憶部808からの指示を受け、カウンタ810が記憶している数値と指定回数記憶部809が記憶している数値とを読み出し、比較する。カウンタ810が記憶している数値が、指定回数記憶部809が記憶している数値よりも大きい場合、比較部811は、セキュリティヒューズ812に対して、フラグを「0」に書き換える信号を出力する。

【0150】

セキュリティヒューズ812は、セキュリティヒューズ708と同様に「0」又は「1」に設定されたフラグであって、「0」は、セキュリティヒューズが切断された状態であり、バッファ813の出力を抑制することを示す。「1」は、バッファ813は通常通りに出力することを示す。セキュリティヒューズ813は、初期状態ではフラグは、「1」に設定されている。セキュリティヒューズ813は、比較部811から指示を受けてフラグを「1」から「0」へ書き換える

。なお、「1」から「0」に書き換えられたフラグを再度「1」に書き換えることは出来ない。

【0151】

<動作>

ここでは、図22及び図20に示すフローチャートを用いて、デバッグシステム8の動作について説明する。

ホストPC82のキーコード入力部823は、不揮発性メモリ805の判定フラグの状態を読み出し（ステップS801）、不揮発性メモリ805にキーコードが書き込み済みか否か判断する。キーコードが書き込み済みの場合（ステップS802でYES）、キーコード入力部823は、ユーザからキーコードの入力を受け付ける（ステップS803）。キーコード入力部823は、受け付けたキーコードを記憶する（ステップS804）。

【0152】

続いて、キーコード入力部823は、受け付けたキーコードを、デバッグユニット80、バッファ813及びデバッグインターフェース807を介して、前回キーコード記憶部808へ送出手する。前回キーコード記憶部808は、内部に記憶している前回キーコードを読む（ステップS805）。前回キーコード記憶部808は、受け付けたキーコードが前回キーコードに一致するか否か判断する。一致しない場合（ステップS806でNO）、前回キーコード記憶部808は、カウンタ810へ信号を出力する。カウンタ810は、前回キーコード記憶部808からの信号を受けて、記憶している数値に1を加算する（ステップS807）。次に、比較部811は、カウンタ810が記憶している数値と指定回数記憶部809が記憶している指定回数とを読み出し、比較する。カウンタ810が記憶している値が、指定回数よりも大きい場合（ステップS808でYES）、比較部811は、セキュリティヒューズ812のフラグを「1」から「0」に書き換える指示を出力し、セキュリティヒューズを切断する（ステップS809）。カウンタ810が記憶している値が、指定回数よりも小さい場合（ステップS808でNO）、ステップS803に戻り処理を続ける。

【0153】

不揮発性メモリ 805 から読み出した判定フラグを判断し、キーコードが書き込み済みでない場合（ステップ S802 で NO）、図 20 のステップ S721 に続く。

前回キーコード記憶部 808 が、受け付けたキーコードが、内部に記憶している前回キーコードに一致する場合（ステップ S806 で YES）、図 20 のステップ S725 に続く。

【0154】

6. 第 6 の実施の形態

本発明に係る第 6 の実施の形態として、デバッグシステム 9 について、図面を参照して説明する。

<構成>

ここでは、デバッグシステム 9 の構成について説明する。デバッグシステム 9 は、マイクロプロセッサ 90、デバッグユニット 91 及びホスト PC 92 から構成される。マイクロプロセッサ 90 は、ユーザが開発する IC カードの基板上に搭載されて接続されており、デバッグユニット 91 は、ケーブルを介してマイクロプロセッサ 90 及びホスト PC 92 と接続されている。

【0155】

ホスト PC 92 は、表示部及びデバッグ部から構成され、デバッグ部は、更に、キーコード入力部、コマンド入力部、復号部及び命令・データ入力部から構成される。なお、ホスト PC 92 の構成は図示していない。ホスト PC 92 の各構成要素は、第 1 の実施の形態におけるホスト PC 12 の各構成要素と同様の機能を有するため説明を省略する。

【0156】

以下では、マイクロプロセッサ 90 の構成について説明する。

図 23 は、マイクロプロセッサ 90 の構成を示すブロック図である。マイクロプロセッサ 90 は、命令メモリ 901、命令実行ユニット 902、データメモリ 903、データ処理ユニット 904、不揮発性メモリ 905、暗号化回路 906、デバッグインターフェース 907 及びセレクタ 908 から構成される。命令メモリ 901、命令実行ユニット 902、データメモリ 903、データ処理ユニッ

ト 904、不揮発性メモリ 905、暗号化回路 906 及びデバッグインターフェース 907 は、それぞれ、第 1 の実施の形態におけるマイクロプロセッサ 10 の命令メモリ 101、命令実行ユニット 102、データメモリ 103、データ処理ユニット 104、不揮発性メモリ 105、暗号化回路 106 及びデバッグインターフェース 107 と同様の機能を有するため、ここでは説明を省略する。

【0157】

セレクトア 908 は、バスを介して不揮発性メモリ 905 と接続されている。更に、セレクトア 908 は、バス A1 を介して命令メモリ 901 と接続され、バス A2 を介してデータメモリ 903 と接続されている。また、セレクトア 908 は、暗号化バス B1 及び暗号化バス B2 を介して暗号化回路 906 と接続されている。暗号化バス B1 は、命令の読み出し及び書き込みに用いるバスであり、暗号化回路 906 と命令メモリ 901 とを接続する。暗号化バス B2 は、データの読み出し及び書き込みに用いるバスであり、暗号化回路 906 とデータメモリ 903 とを接続する。

【0158】

セレクトア 908 は、不揮発性メモリ 905 の判定フラグを読み出して判定フラグの状態に応じて、以下に示す様にバスを選択する。

不揮発性メモリ 905 に判定フラグが書き込まれていない場合、すなわち、不揮発性メモリ 905 にキーコードが書き込まれていない場合、セレクトア 908 は、命令読み出し処理及び命令書き込み処理においては、バス A1 を選択する。命令読み出し処理では、セレクトア 908 は、バス A1 を介して命令メモリ 901 から命令を読み出し、読み出した命令をデバッグインターフェース 907 へ出力する。命令書き込み処理では、セレクトア 908 は、デバッグインターフェース 907 から命令を受け取り、受け取った命令をバス A1 を介して命令メモリ 901 へ書き込む。データ読み出し処理及びデータ書き込む処理においては、バス A2 を選択する。データ読み出し処理では、セレクトア 908 は、バス A2 を介してデータメモリ 903 からデータを読み出し、読み出したデータをデバッグインターフェース 907 へ出力する。データ書き込み処理では、セレクトア 908 は、デバッグインターフェース 907 からデータを受け取り、受け取ったデータをバス A1

を介して命令メモリ 901 へ書き込む。

【0159】

不揮発性メモリ 905 に判定フラグが書き込まれている場合、すなわち、不揮発性メモリ 905 にキーコードが書き込み済みの場合、セレクタ 908 は命令読み出し処理においては、暗号化バス B1 を選択する。セレクタ 908 は、暗号化バス B1 を介して命令メモリ 901 から命令を読み出し、読み出した命令を暗号化回路 906 へ出力する。セレクタ 908 は、暗号化バス B1 を介して暗号化回路 906 から暗号化命令を受け取り、受け取った暗号化命令をデバッグインターフェース 907 へ出力する。セレクタ 908 は、命令書き込み処理においては、バス A1 を選択する。セレクタ 908 は、デバッグインターフェース 907 から命令を受け取り、受け取った命令をバス A1 を介して命令メモリ 901 へ書き込む。セレクタ 908 は、データ読み出し処理においては、暗号化バス B2 を選択する。セレクタ 908 は、暗号化バス B2 を介してデータメモリ 903 からデータを読み出し、読み出したデータを暗号化回路 906 へ出力する。セレクタ 908 は、暗号化バス B2 を介して暗号化回路 906 から暗号化データを受け取り、受け取った暗号化データをデバッグインターフェース 907 へ出力する。セレクタ 908 は、データ書き込み処理においては、バス A2 を選択する。セレクタ 908 は、デバッグインターフェース 907 からデータを受け取り、受け取ったデータをバス A2 を介してデータメモリ 903 へ書き込む。

【0160】

これにより、不揮発性メモリ 905 にキーコードが書き込み済みの場合は、暗号化回路 906 により暗号化された暗号化命令及び暗号化データが、デバッグインターフェース 907 及びデバッグユニット 91 を介してホスト PC 92 へ送出され、不揮発性メモリ 905 にキーコードが書き込み済みでない場合は、暗号化されていない命令及びデータが、デバッグインターフェース 907 及びデバッグユニット 91 を介してホスト PC 92 へ送出される。

【0161】

<動作>

ここでは、図 24、図 25 及び図 4 に示すフローチャートを用いてデバッグシ

ステム 9 の動作について説明する。

ホスト PC 92 のデバッグ部が起動し、デバッグ部からの信号を受けて、マイクロプロセッサ 90 のデバッグインターフェース 907 は、不揮発性メモリ 905 の判定フラグの状態を読み出し（ステップ S 901）、不揮発性メモリ 905 にキーコードが書き込み済みか否かを判断する。

【0162】

キーコードが書き込み済みの場合（ステップ S 902 で YES）、ホスト PC 92 のキーコード入力部は、ユーザからキーコードの入力を受け付け（ステップ S 909）、受け付けたキーコードを、デバッグユニット 91 を介してデバッグインターフェース 907 へ送出し、ステップ S 907 へ続く。キーコードが書き込み済みでない場合（ステップ S 902 で NO）、デバッグインターフェース 907 は、キーコードが書き込み済みでないことを示す信号を、デバッグユニット 91 を介してホスト PC 92 のデバッグ部へ送出する。

【0163】

デバッグ部は、キーコードを不揮発性メモリ 905 に書き込むか否かをユーザに問うための画面を表示部へ出力し、当該画面が表示されている状態に於いて、デバッグ部のキーコード入力部は、ユーザからの選択を受け付ける。キーコードを書き込まない選択を受け付けた場合（ステップ S 903 で NO）、図 25 のフローチャートに続く。

【0164】

ホスト PC 92 のコマンド入力部が、ユーザからコマンドの入力を受け付ける（ステップ S 910）。ここで、コマンドの種類は、「命令表示」、「命令書込み」、「データ表示」、「データ書込み」及び「終了」であり、これらの内の何れかがユーザにより選択される。コマンド入力部は、選択されたコマンドを判断する（ステップ S 911）。

【0165】

コマンドが「命令表示」であれば（ステップ S 911 で「命令表示」）、デバッグ部は、デバッグユニット 91 を介して、デバッグインターフェース 907 へコマンドに対応する信号を送出する。デバッグインターフェース 907 は、命令

メモリから命令を読み出し（ステップS912）、セクタ908は、バスA1を選択して命令をデバッグインターフェース907及びデバッグユニット91を介してホストPC92へ出力する（ステップS913）。ホストPC92の表示部は、命令を受け取り、受け取った命令を画面に表示する（ステップS914）。その後、ステップS910に戻り処理を続ける。

【0166】

コマンドが「命令書込み」であれば（ステップS911で「命令書込み」）、ホストPC92の命令・データ入力部は、ユーザから命令の入力を受け付ける（ステップS921）。命令・データ入力部は、受け付けた命令を、デバッグユニット91を介してデバッグインターフェース907へ出力する（ステップS922）。セクタ908は、バスA1を選択し、デバッグインターフェース907は、バスA1を介して命令を命令メモリ901に書き込む（ステップS923）。その後、ステップS910に戻り処理を続ける。

【0167】

コマンドが「データ表示」であれば（ステップS911で「データ表示」）、デバッグ部は、デバッグユニット91を介してデバッグインターフェース907へコマンドに対応する信号を出力する。デバッグインターフェース907は、データメモリ903からデータを読み出し（ステップS931）、セクタ908は、バスA2を選択してデータをデバッグインターフェース907及びデバッグユニット91を介してホストPC92へを出力する（ステップS932）。ホストPC92の表示部は、データを受け取り、受け取ったデータを画面に表示する（ステップS933）。その後、ステップS910に戻り処理を続ける。

【0168】

コマンドが「データ書込み」であれば（ステップS911で「データ書込み」）、ホストPC92の命令・データ入力部は、ユーザからデータの入力を受け付ける（ステップS941）。命令・データ入力部は、受け付けたデータを、デバッグユニット91を介してデバッグインターフェース907へ出力する。（ステップS942）。セクタ908は、バスA2を選択して、デバッグインターフェース907は、バスA2を介してデータをデータメモリ903に書き込む（ス

テップS943)。その後、ステップS910に戻り処理を続ける。

【0169】

コマンドが「終了」であれば（ステップS911で「終了」）、処理を終了する。

ここで、図24のステップS903に戻る。キーコードを書き込む場合（ステップS903でYES）、キーコード入力部は、ユーザからキーコードの入力を受け付け（ステップS904）、受け付けたキーコードを、内部に記憶すると共に、デバッグユニット91を介してデバッグインターフェース907へ送出する。デバッグインターフェース907は、キーコードを受け取り、受け取ったキーコードを不揮発性メモリ905に書き込む（ステップS905）。更に、デバッグインターフェース907は、キーコードが書き込み済みであることを示す判定フラグを不揮発性メモリ905に書き込む（ステップS906）。

【0170】

次に、ホストPC92のコマンド入力部が、ユーザからコマンドの入力を受け付ける（ステップS907）。ここで、コマンドの種類は、「命令表示」、「命令書込み」、「データ表示」、「データ書込み」及び「終了」であり、これらの内の何れかがユーザにより選択される。コマンド入力部は、選択されたコマンドを判断する（ステップS908）。

【0171】

以下は、図4に示した第1の実施の形態におけるデバッグシステム1の動作と同様の処理であるため、ここでは図4のフローチャートを用いてデバッグシステム1との相違点を中心に説明する。

コマンドが「命令表示」であれば（ステップS908で「命令表示」）、デバッグインターフェース907は、命令メモリ901から命令を読み出し（ステップS109）、セクタ908は、暗号化バスB1を選択して命令を暗号化回路906へ出力する。暗号化回路906は、命令に暗号化処理を施し暗号化命令を生成する（ステップS110）。暗号化回路906は、生成した暗号化命令を、暗号化バスB1を介してデバッグインターフェース907へ出力し、デバッグインターフェース907は、デバッグユニット91を介して暗号化命令をホストP

C92へ出力する（ステップS111）。以下は、デバッグシステム1と同様である。

【0172】

コマンドが「命令書込み」であれば（ステップS908で「命令書込み」）、ホストPC92の命令・データ入力部は、ユーザから命令の入力を受け付ける（ステップS121）。命令・データ入力部は、受け付けた命令を、デバッグユニット91を介してデバッグインターフェース907へ出力する（ステップS122）。セレクタ908は、バスA1を選択して、デバッグインターフェース907は、バスA1を介して命令を命令メモリ901に書き込む（ステップS123）。その後、ステップS907に戻り処理を続ける。

【0173】

コマンドが「データ表示」であれば（ステップS908で「データ表示」）、デバッグインターフェース907は、データメモリ903からデータを読み出し（ステップS131）、セレクタ908は、暗号化バスB2を選択して読み出したデータを暗号化回路906へ出力する。暗号化回路906は、データに暗号化処理を施して暗号化データを生成する（ステップS132）。暗号化回路906は、生成した暗号化データを、暗号化バスB2を介してデバッグインターフェース907へ出力し、デバッグインターフェース907は、デバッグユニット91を介して暗号化データをホストPC92へ出力する（ステップS133）。以下は、デバッグシステム1と同様である。

【0174】

コマンドが「データ書込み」であれば（ステップS908で「データ書込み」）、ホストPC92の命令・データ入力部は、ユーザからデータの入力を受け付ける（ステップS141）。命令・データ入力部は、受け付けたデータを、デバッグユニット91を介してデバッグインターフェース907へ出力する（ステップS142）。セレクタ908は、バスA2を選択し、デバッグインターフェース907はバスA2を介してデータをデータメモリ903に書き込む（ステップS143）。その後、ステップS907に戻り処理を続ける。

【0175】

コマンドが「終了」であれば（ステップS908で「終了」）、処理を終了する。

7. 第7の実施の形態

本発明に係る第7の実施の形態として、デバッグシステム15について図面を参照して説明する。

【0176】

デバッグシステム15は、マイクロプロセッサ100、デバッグユニット110及びホストPC120から構成される。マイクロプロセッサ100は、ユーザが開発するICカードの基板上に搭載されて接続されており、デバッグユニット110は、ケーブルを介してマイクロプロセッサ100及びホストPC120と接続されている。

【0177】

（マイクロプロセッサ100の構成）

図25は、マイクロプロセッサ100の構成を示すブロック図である。同図に示す様に、マイクロプロセッサ100は、命令メモリ1001、命令実行ユニット1002、データメモリ1003、データ処理ユニット1004、不揮発性メモリ1005、復号化回路1006、デバッグインターフェース1007及びキャッシュ1008から構成される。

【0178】

マイクロプロセッサ100は、復号化回路1006と命令実行ユニット1002との間にキャッシュ1008を有することが特徴である。命令メモリ1001、命令実行ユニット1002、データメモリ1003、データ処理ユニット1004、不揮発性メモリ1005、復号化回路1006及びデバッグインターフェース1007は、それぞれ、第2の実施の形態におけるマイクロプロセッサ20の各構成要素と同様の機能を有する。以下ではマイクロプロセッサ20との相違点を中心に説明する。

【0179】

キャッシュ1008は、復号化回路1006と命令実行ユニット1002との間に設けられたキャッシュメモリであって、命令実行ユニット1003における

命令の実行時間が、復号化回路 1006 における暗号化命令の復号処理よりも長い場合に、命令実行ユニット 1002 における命令の実行中に復号化回路 1006 から受け取る命令を内部に蓄積する。

【0180】

命令実行ユニット 1002 は、キャッシュ 1008 が蓄積している命令を読み出して、読み出した命令を実行する。

デバッグシステム 15 の動作については、デバッグシステム 2 と同様であるため、説明を省略する。

8. まとめ

以上説明したように、本発明のデバッグシステム及びマイクロプロセッサによれば、デバッガが起動するホスト PC 上でユーザから入力されたキーコードを用いて、マイクロプロセッサとホスト PC との間で命令及びデータを暗号化して伝送することができる。本発明のデバッグシステム及びマイクロプロセッサによれば、悪意のあるユーザがマイクロプロセッサをデバッグユニットに接続してマイクロプロセッサを解析しようとしても、マイクロプロセッサから取得できるのは、暗号化命令及び暗号化データであり、暗号化命令及び暗号化データを取得した場合であっても、マイクロプロセッサの不揮発性メモリに記憶されている正しいキーコードを知らなければ復号することができず、マイクロプロセッサの内部情報を解析することができない。更に、マイクロプロセッサ設計者、デバッグシステム設計者、プログラム開発者なども正しいキーコードを知ることはなく、キーコード設定者のみがマイクロプロセッサの内部情報を解析することができる。これにより、課金処理を行うような、高度なセキュリティが要求されるシステムにおいてもデバッグとセキュリティの維持を両立することができる。

【0181】

以上、本発明を上記実施の形態に基づき説明してきたが、本発明は上記実施の形態に限定されず、以下のような場合も本発明に含まれる。

(1) 上記実施の形態において、デバッグの対象であるマイクロプロセッサは、IC カードの基板上に搭載されているが、IC カードの基板に限定されないのは勿論であり、ユーザが開発するターゲット基板であればよい。

【0182】

(2) 上記実施の形態では、デバッガのコマンドは、「命令表示」、「命令書込み」、「データ表示」、「データ書込み」及び「終了」であるが、本発明において、デバッガのコマンドは、これらに限定されない。

(3) 第2の実施の形態における命令書込み処理は、デバッグ部222の命令・データ入力部228が受け付けた命令を暗号化してマイクロプロセッサ20の命令メモリ201に格納しているが、デバッグ部222は、外部記憶装置に記憶されているソースファイルを指定し、コンパイル部224が指定されたソースファイルを読み込み、オブジェクトファイルを生成し、生成したオブジェクトファイルを、暗号化して、暗号化オブジェクトファイルをマイクロプロセッサ20の命令メモリ201に格納する構成としてもよい。また、予めコンパイル部224が、暗号化した暗号化オブジェクトを外部記憶装置へ格納しておき、デバッグ部222は、外部記憶装置に格納されている暗号化オブジェクトファイルを読み出してマイクロプロセッサ20の命令メモリ201に書き込むように構成してもよい。

【0183】

(4) また、第2の実施の形態において、不揮発性メモリ205が保持するキーコードは、読み出しが不可能であり、且つ、書き換えが可能であっても良い。この場合、コンパイラで指定したキーコードが分からない限り、不揮発性メモリ205が保持するキーコードを書き換えても、命令が正常に実行できなくなり、セキュリティ上の問題は無い。

【0184】

(5) また、第2の実施の形態<変形例3>において、メモリリードライト装置51の対象は、マイクロプロセッサ50に限定されない。例えば、マイクロプロセッサ50の外部に接続されたメモリもメモリリードライト装置51の対象になる。

(6) また、第3の実施の形態では、デバッグを行う複数の者に対して、予め固有のキーコードとキーコード番号とが秘匿に通知されているとしてもよい。任意のキーコードを入力するのではなく、予め他人には秘匿に設定されて保持され

たキーコードを用いる構成も本発明に含まれる。

【0185】

また、キーコードの数とメモリブロックの数とは1対1に対応していなくてもよい。秘匿したいレベルに応じた数のキーコードによりメモリが管理される構成であれば、1個のキーコードが複数のメモリブロックに対応する構成も本発明に含まれる。

(7) 命令及びデータの暗号化に用いる暗号アルゴリズムはDESに限定されない。公開鍵暗号方式であってもよい。

【0186】

(8) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD-ROM、DVD-RAM、半導体メモリ等に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は、前記デジタル信号を電気通信回路、無線又は有線通信回路、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

【0187】

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、前記コンピュータプログラムを記憶しており、前記マイクロプロセッサが前記コンピュータプログラムに従って動作するとしてもよい。

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は、前記プログラム又は前記デジタル信号をネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

【0188】

(9) 第1の実施の形態から第7の実施の形態を適宜組み合わせた構成も本発明に含まれる。また、各実施の形態に上記変形例を組み合わせた構成も本発明に含まれる。

【0189】

【発明の効果】

以上説明したように、本発明は、外部に秘匿するプログラム情報を記憶しているマイクロプロセッサと、前記マイクロプロセッサと接続され、前記マイクロプロセッサの動作をデバッグするために用いられるホストコンピュータとから構成されるデバッグシステムである。

【0190】

前記マイクロプロセッサは、前記プログラム情報をセキュアに扱うために用いられる鍵情報を記憶する為の領域を備える一度だけ書き込みが可能な不揮発性メモリを備え、前記不揮発性メモリが鍵情報を記憶していない場合に、前記ホストコンピュータから鍵情報を受け取り、受け取った鍵情報を前記不揮発性メモリに書き込み、前記不揮発性メモリが記憶している鍵情報を用いて、前記ホストコンピュータとの間で前記プログラム情報をセキュアに伝送する。

【0191】

前記ホストコンピュータは、利用者から鍵情報の入力を受け付け、前記鍵情報を内部に記憶すると共に、前記マイクロプロセッサへ送出し、記憶している前記鍵情報を用いて、前記マイクロプロセッサとの間で前記プログラム情報をセキュアに伝送する。

この構成によると、前記不揮発性メモリに書き込まれた鍵情報は、読み出し及び書き換えが不可能である。前記デバッグシステムにおいて、前記マイクロプロセッサ及び前記ホストコンピュータは、読み出し及び書き換えが不可能な鍵情報を用いて前記プログラム情報をセキュアに伝送するため、前記ホストコンピュータから初めて鍵情報を入力した利用者のみが、前記マイクロプロセッサのプログラム情報を取得することが出来る。それにより、前記マイクロプロセッサを用いるシステムの開発段階において、複数の開発者が関わる場合であっても、前記利用者のみが前記マイクロプロセッサのプログラム情報を取得して、セキュリティ

を保ちつつデバッグすることができる。

【0192】

また、本発明は、デバッグするために用いられるホストコンピュータと接続され、外部に秘匿するプログラム情報を記憶しているマイクロプロセッサである。前記マイクロプロセッサは、プログラム、データ又はプログラム及びデータを示す前記プログラム情報を記憶しており、前記プログラム情報を読み出し、読み出したプログラム情報に従って動作する。前記マイクロプロセッサは、前記プログラム情報をセキュアに扱うために用いられる鍵情報を記憶する為の領域を備える。一度だけ書き込みが可能な不揮発性メモリを備え、前記不揮発性メモリが鍵情報を記憶していない場合に、前記ホストコンピュータから鍵情報を受け取り、受け取った鍵情報を前記不揮発性メモリに書き込み、前記不揮発性メモリが記憶している鍵情報を用いて、前記ホストコンピュータとの間で前記プログラム情報をセキュアに伝送する。

【0193】

この構成によると、前記マイクロプロセッサの前記不揮発性メモリが記憶する鍵情報は、一度書き込まれると読み出し及び書き換えが不可能であるため、前記マイクロプロセッサは、接続されたホストコンピュータとの間で、前記プログラム情報をセキュアに伝送することができる。

ここで、前記不揮発性メモリは、鍵情報が書き込み済みか否かを示すフラグ情報を記憶しており、前記マイクロプロセッサは、前記フラグ情報を読み出し、読み出した前記フラグ情報が前記不揮発性メモリに鍵情報が書き込まれていないことを示す場合に、前記ホストコンピュータから鍵情報を受け付け、受け付けた鍵情報を前記不揮発性メモリに書き込むように構成してもよい。

【0194】

この構成によると、前記伝送手段は、前記不揮発性メモリのフラグを読み出すことにより、前記不揮発性メモリに鍵情報が書き込まれているか否かを判断することができる。

ここで、前記マイクロプロセッサは、前記不揮発性メモリに記憶されている鍵情報を用いて、前記プログラム情報を暗号化し、暗号化されたプログラム情報を

出力するように構成してもよい。

【0195】

この構成によると、プログラム情報を暗号化するために用いる鍵情報は、前記不揮発性メモリが記憶している鍵情報である。前記不揮発性メモリが記憶している鍵情報は、前述の通り、一度だけ書き込みが可能で読み出し及び書き換えが出来ない。そのため前記マイクロプロセッサは、セキュリティの高い状態でプログラム情報を前記ホストコンピュータへ伝送することが可能である。

【0196】

ここで、前記マイクロプロセッサは、前記プログラム、データ又はプログラム及びデータが鍵情報を用いて暗号化されて生成されたプログラム情報を記憶しており、前記不揮発性メモリから鍵情報を読み出し、読み出した鍵情報を用いて、プログラム情報を復号してプログラム、データ又はプログラム及びデータを生成し、生成したプログラム、データ又はプログラム及びデータに従って動作し、プログラム、データ又はプログラム及びデータが暗号化されて生成されたプログラム情報を前記ホストコンピュータへ伝送するように構成してもよい。

【0197】

この構成によると、前記マイクロプロセッサは、既に暗号化されたプログラム情報を記憶しているため、前記ホストコンピュータとの間でセキュリティを保った状態でプログラム情報を伝送することができる。更に、暗号化されたプログラム情報を実行する場合は、暗号化されたプログラム情報を、前記不揮発性メモリが記憶している鍵情報を用いて復号することで、プログラム情報記憶手段がプログラム情報を暗号化した状態で記憶していてもプログラムを実行することができる。

【0198】

ここで、前記マイクロプロセッサは、更に、動作の結果生成された生成データを、鍵情報を用いて暗号化し、暗号化された生成データを内部に書き込むように構成してもよい。

この構成によると、前記不揮発性メモリが暗号化されたデータを記憶している場合であっても、暗号化されたデータを、鍵情報を用いて復号し、演算後のデー

タを再度鍵情報を用いて暗号化することでプログラム情報のセキュリティを保ちつつプログラム情報を実行することができる。

【0199】

ここで、前記マイクロプロセッサは、前記プログラムのみが鍵情報を用いて暗号化された暗号化プログラムを含むプログラム情報を記憶しており、前記外部装置との通信経路を備えるように構成してもよい。

この構成によると、前記プログラム情報記憶部は外部装置と接続されているがプログラムは暗号化されているため、プログラムのセキュリティは保たれる。データは暗号化されていないため、必要に応じて外部装置からデータを取得することが可能である。

【0200】

ここで、前記鍵情報は1以上の部分鍵情報から構成され、前記プログラムは、複数の部分プログラムから構成され、各部分プログラムは、前記1以上の部分鍵情報の何れかに対応しており、前記マイクロプロセッサは、複数の部分プログラムが、対応する部分鍵情報を用いて暗号化された暗号化部分プログラムを含むプログラム情報を記憶しており、前記不揮発性メモリから部分鍵情報を読み出し、読み出した部分鍵情報に対応する1以上の暗号化部分プログラムを読み出し、読み出した1以上の暗号化部分プログラムを、前記部分鍵情報を用いて復号して部分プログラムを生成し、生成した部分プログラムに従って動作するように構成してもよい。

【0201】

この構成によると、部分プログラム毎に異なる鍵情報が設定されており、複数の開発者がそれぞれ互いに知ることのない鍵情報を設定することで部分プログラム毎にセキュリティを保った状態で前記ホストコンピュータへ伝送が可能である。

ここで、前記マイクロプロセッサは、さらに、前記ホストコンピュータからの要求に応じて、暗号化されたプログラム情報の出力を抑制するように構成してもよい。

【0202】

この構成によると、プログラム情報が暗号化された状態であっても、前記ホストコンピュータからの要求により前記ホストコンピュータへのプログラム情報の出力を抑制することができるため、悪意のある解析者が前記ホストコンピュータからプログラム情報を取得するのを防止することができる。

ここで、前記マイクロプロセッサは、さらに、鍵情報に係る情報であり、暗号化されたプログラム情報の出力の抑制を示す抑制条件を記憶しており、前記ホストコンピュータから受け付けた前記鍵情報が、前記抑制条件を満たす場合に、暗号化されたプログラム情報の出力を抑制するように構成してもよい。

【0203】

この構成によると、プログラム情報が暗号化された状態であっても、前記鍵情報が前記抑制条件を満たす場合に、前記ホストコンピュータへのプログラム情報の出力を抑制することができるため、悪意のある解析者が前記ホストコンピュータからプログラム情報を取得するのを防止することができる。ここで、上述のマイクロプロセッサと比較すると、上述のマイクロプロセッサは、ホストコンピュータからの指示を受けてプログラム情報の出力を抑制するのに対し、当該マイクロプロセッサは、出力を抑制するための判断を当該マイクロプロセッサ自身が行うため、よりセキュリティが高い。

【0204】

ここで、前記不揮発性メモリは、鍵情報が書き込み済みか否かを示すフラグ情報を記憶しており、前記マイクロプロセッサは、前記フラグ情報を読み出し、読み出したフラグ情報が前記不揮発性メモリに鍵情報が書き込まれていないことを示す場合に、前記プログラム情報を読み出し、読み出したプログラム情報を出力し、読み出したフラグ情報が前記不揮発性メモリに鍵情報が書き込まれていることを示す場合に、前記プログラム情報を読み出し、読み出したプログラム情報を前記鍵情報で暗号化し、暗号化されたプログラム情報を出力するように構成してもよい。

【0205】

この構成によると、前記マイクロプロセッサは、前記プログラム情報を暗号化して出力するか、暗号化せずに出力するかを選択することができる。それにより

、前記不揮発性メモリに鍵情報が記憶されていない状態において、プログラム開発者はプログラム情報を暗号化せずにデバッグを行い、その後、他の利用者が鍵情報を設定することができる。これを、ICカードを用いたサービスシステムの例を用いて説明する。ICカードに搭載されるマイクロプロセッサの開発者、プログラム開発者及びICカード開発者は、開発段階においてプログラム情報を暗号化せず取得し、デバッグを行うことができる。その後、ICカードを用いたサービス業者がプログラム情報を書き込み、更に、前記不揮発性メモリに鍵情報を書き込む。これ以後は、当該サービス業者のみがプログラム情報を取得することができる。

【0206】

ここで、前記マイクロプロセッサは、更に、キャッシュメモリを備える、前記マイクロプロセッサは、前記プログラム、データ又はプログラム及びデータが鍵情報を用いて暗号化されて生成されたプログラム情報を記憶しており、前記不揮発性メモリから鍵情報を読み出し、読み出した鍵情報を用いて、プログラム情報を復号してプログラム、データ又はプログラム及びデータを生成し、生成した前記プログラム、データ又はプログラム及びデータを前記キャッシュメモリに書き込む。前記マイクロプロセッサは、実行ユニットにおける実行速度に応じて前記キャッシュメモリから前記プログラム、データ又はプログラム及びデータを読み出し、読み出したプログラム、データ又はプログラム及びデータに従って動作する。前記マイクロプロセッサは、プログラム、データ又はプログラム及びデータが暗号化されて生成されたプログラム情報を前記ホストコンピュータに伝送するように構成してもよい。

【0207】

この構成によると、前記実行手段における復号処理時間が長く、実行処理時間が短い場合であっても、復号したプログラムを前記キャッシュメモリに蓄積することにより実行処理をスムーズに継続することができる。

また、本発明は、外部に秘匿するプログラム情報を記憶しているマイクロプロセッサと接続され、前記マイクロプロセッサの動作をデバッグするホストコンピュータである。前記ホストコンピュータは、利用者から鍵情報の入力を受け付け

、前記鍵情報を、内部に記憶すると共に前記マイクロプロセッサへ送出し、記憶している前記鍵情報を用いて、前記マイクロプロセッサとの間で前記プログラム情報をセキュアに伝送することを特徴とする。

【0208】

この構成によると利用者から受け付けた鍵情報を前記マイクロプロセッサへ送出し、当該鍵情報を用いて前記プログラム情報を伝送するので、当該利用者以外の者に対してセキュリティが保たれる。

ここで、前記ホストコンピュータは、前記マイクロプロセッサから、前記鍵情報を用いて暗号化されたプログラム情報を受け取り、前記暗号化されたプログラム情報に、記憶している前記鍵情報を用いて復号し、復号したプログラム情報を表示するように構成してもよい。

【0209】

この構成によると、前記利用者以外の者が前記プログラム情報を復号することは不可能であり、セキュリティを保った状態で前記利用者は前記プログラム情報を取得し、デバッグを行うことができる。

ここで、前記ホストコンピュータは、更に、利用者から、プログラム、データ又はプログラム及びデータを示すプログラム情報の入力を受け付け、受け付けた前記プログラム情報に、記憶している前記鍵情報を用いて暗号化し、暗号化したプログラム情報を前記マイクロプロセッサへ出力するように構成してもよい。

【0210】

この構成によると、プログラム情報を暗号化して前記マイクロプロセッサに伝送するため、セキュリティを保った状態で前記プログラム情報を前記マイクロプロセッサへ伝送することができる。

ここで、前記ホストコンピュータは、更に、ソースプログラムを記憶しており、前記ソースプログラムを変換してプログラムを示すプログラム情報を生成し、生成した前記プログラム情報に、前記鍵情報を用いて暗号化し、暗号化したプログラム情報を前記マイクロプロセッサへ伝送するように構成してもよい。

【0211】

この構成によると、前記ホストコンピュータがソースプログラムをコンパイル

して、更に、生成したオブジェクトプログラムを暗号化して前記マイクロプロセッサへ伝送するため、セキュリティを保った状態で前記マイクロプロセッサへプログラムを書き込むことができる。

ここで、前記マイクロプロセッサは、更に、鍵情報に係る情報で、前記マイクロプロセッサとの間での、前記暗号化されたプログラム情報の伝送の停止を示す停止条件を記憶しており、受け付けた前記鍵情報が、前記停止条件を満たす場合に、前記マイクロプロセッサに対して、前記暗号化されたプログラム情報の出力を抑制することを示す要求を出力するように構成してもよい。

【0212】

この構成によると、前記ホストコンピュータは、前記停止条件として異なる鍵情報が入力された回数を示す数値を記憶しておき、何度も異なる鍵情報が入力された場合に、前記マイクロプロセッサとの間の暗号化されたプログラム情報の伝送を停止することができる。これにより、何度も異なる鍵情報を入力して暗号化されたプログラム情報を復号しようとする悪意のある者が、プログラム情報を復号して、改竄することを防止することができる。

【図面の簡単な説明】

【図1】

マイクロプロセッサ10の構成を示すブロック図である。

【図2】

ホストPC12の構成を示すブロック図である。

【図3】

デバッグシステム1の動作を示すフローチャートであり、図4に続く。

【図4】

デバッグシステム1の動作を示すフローチャートであり、図3から続く。

【図5】

マイクロプロセッサ20の構成を示すブロック図である。

【図6】

ホストPC22の構成を示すブロック図である。

【図7】

デバッグシステム 2 の動作を示すフローチャートであり、図 3 から続く。

【図 8】

マイクロプロセッサ 30 の構成を示すブロック図である。

【図 9】

マイクロプロセッサ 40 の構成を示すブロック図である。

【図 10】

ホスト PC 42 の構成を示すブロック図である。

【図 11】

デバッグシステム 4 の動作を示すフローチャートであり、図 3 から続く。

【図 12】

ホスト PC 52 の構成を示すブロック図である。

【図 13】

デバッグシステム 5 の動作を示すフローチャートであり、図 3 から続く。

【図 14】

マイクロプロセッサ 60 の構成を示すブロック図である。

【図 15】

ホスト PC 62 の構成を示すブロック図である。

【図 16】

デバッグシステム 6 の動作を示すフローチャートであり、図 7 に続く。

【図 17】

マイクロプロセッサ 70 の構成を示すブロック図である。

【図 18】

ホスト PC 72 の構成を示すブロック図である。

【図 19】

デバッグシステム 7 の動作を示すフローチャートであり、図 4 及び図 20 に続く。

【図 20】

デバッグシステム 7 の動作を示すフローチャートであり、図 19 及び図 22 から続く。

【図 2 1】

マイクロプロセッサ 80 の構成を示すブロック図である。

【図 2 2】

デバッグシステム 8 の動作を示すフローチャートであり、図 4 及び図 2 0 に続く。

【図 2 3】

マイクロプロセッサ 90 の構成を示すブロック図である。

【図 2 4】

デバッグシステム 9 の動作を示すフローチャートであり、図 4 及び図 2 5 に続く。

【図 2 5】

デバッグシステム 9 の動作を示すフローチャートであり、図 2 4 から続く。

【図 2 6】

マイクロプロセッサ 100 の構成を示すブロック図である。

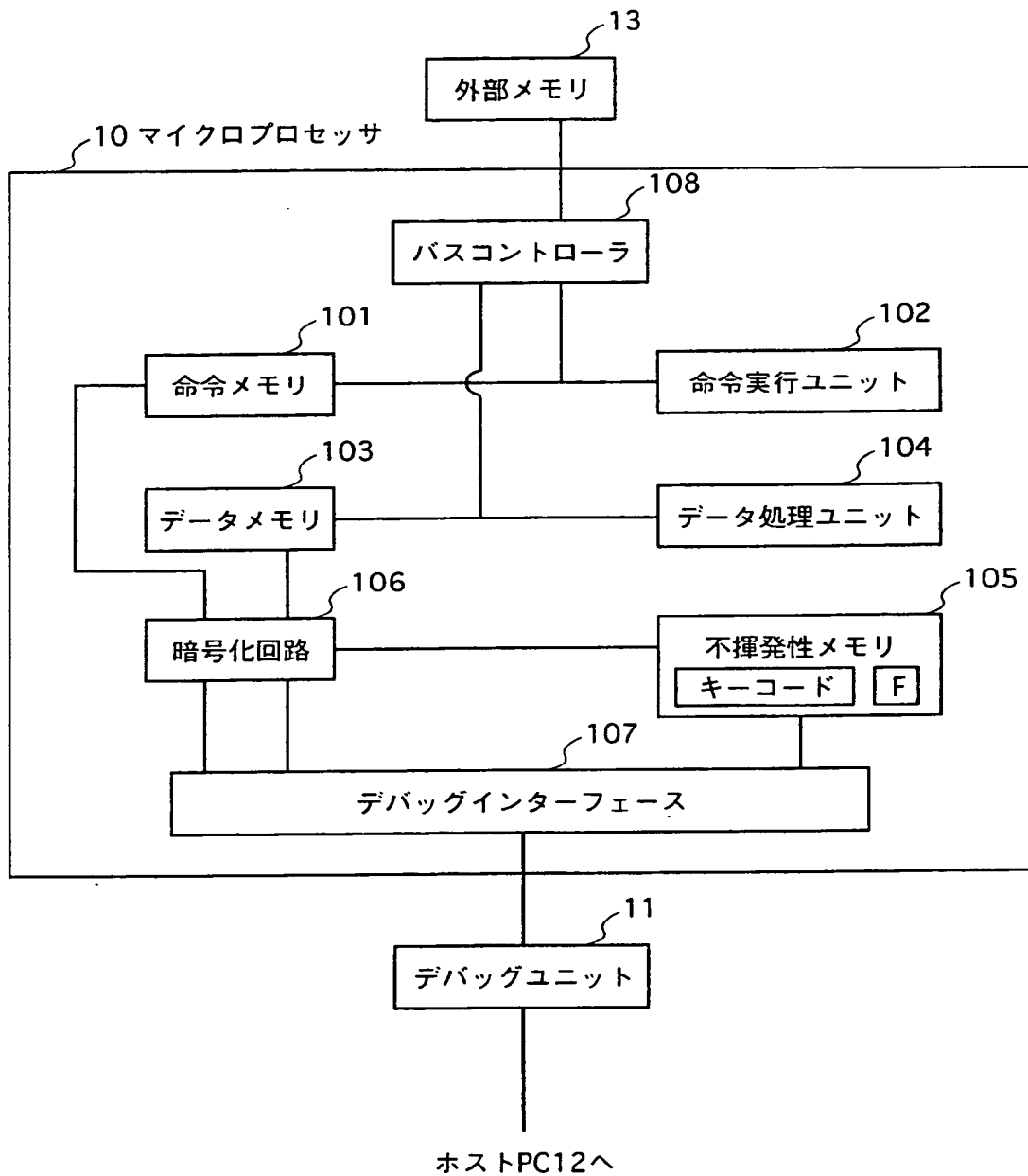
【符号の説明】

- 10 マイクロプロセッサ
- 11 デバッグユニット
- 12 ホスト P C
- 13 外部メモリ
- 20 マイクロプロセッサ
- 21 デバッグユニット
- 22 ホスト P C
- 23 外部メモリ
- 30 マイクロプロセッサ
- 31 デバッグユニット
- 32 ホスト P C
- 33 外部メモリ
- 40 マイクロプロセッサ
- 41 デバッグユニット

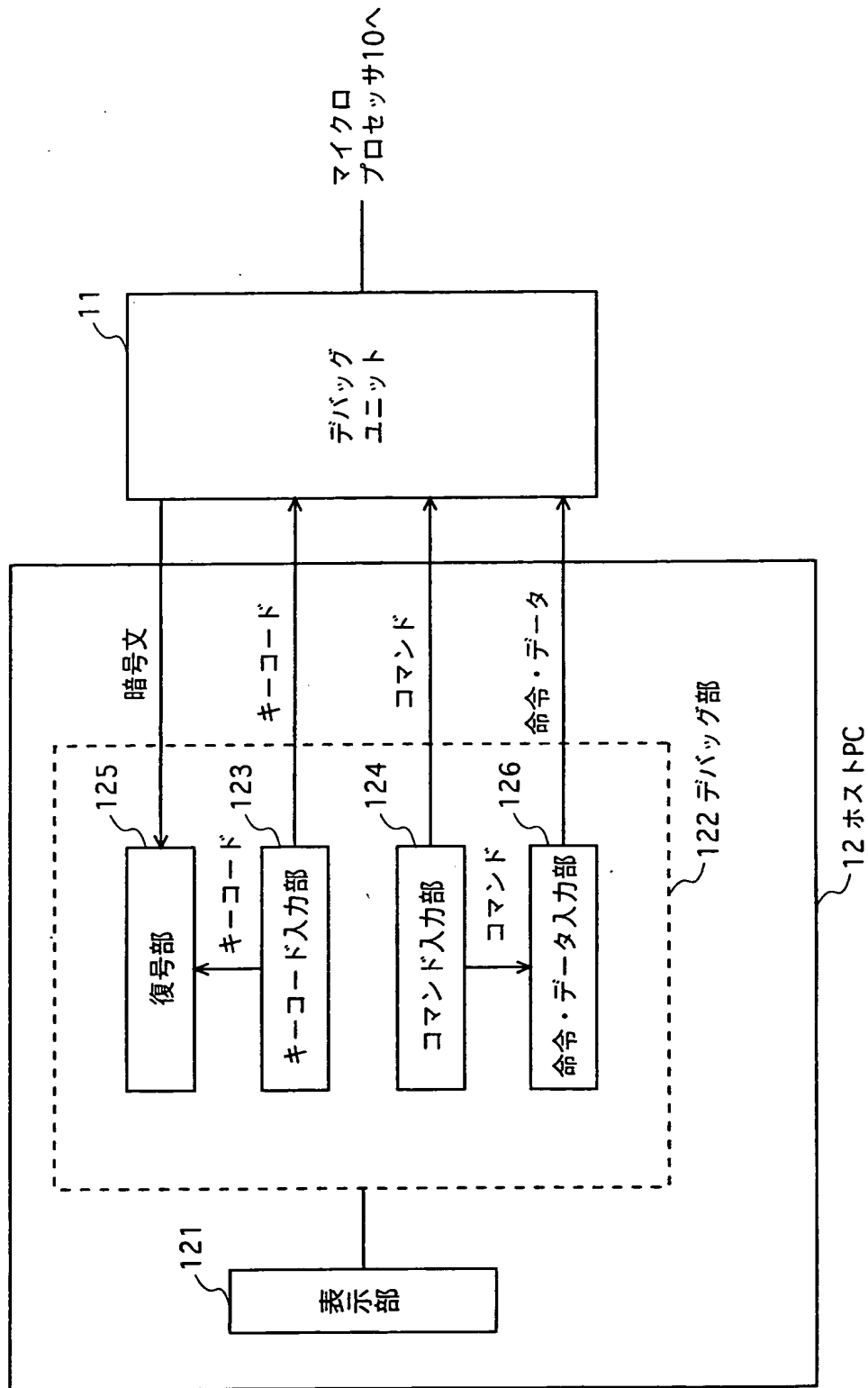
42 ホストPC
50 マイクロプロセッサ
51 メモリリードライト装置
52 ホストPC
60 マイクロプロセッサ
61 デバッグユニット
62 ホストPC
63 外部メモリ
70 マイクロプロセッサ
71 デバッグユニット
72 ホストPC
80 マイクロプロセッサ
81 デバッグユニット
82 ホストPC
90 マイクロプロセッサ
91 デバッグユニット
92 ホストPC
100 マイクロプロセッサ
110 デバッグユニット
120 ホストPC

【書類名】 図面

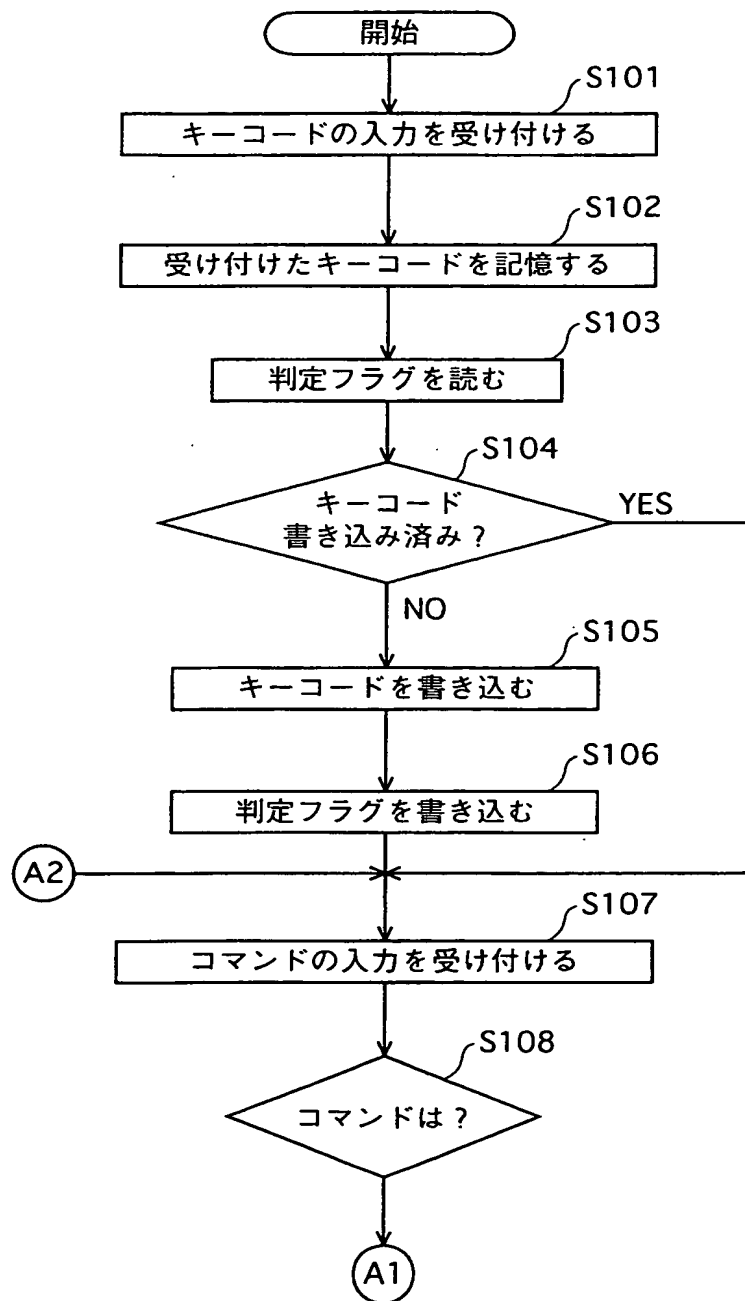
【図 1】



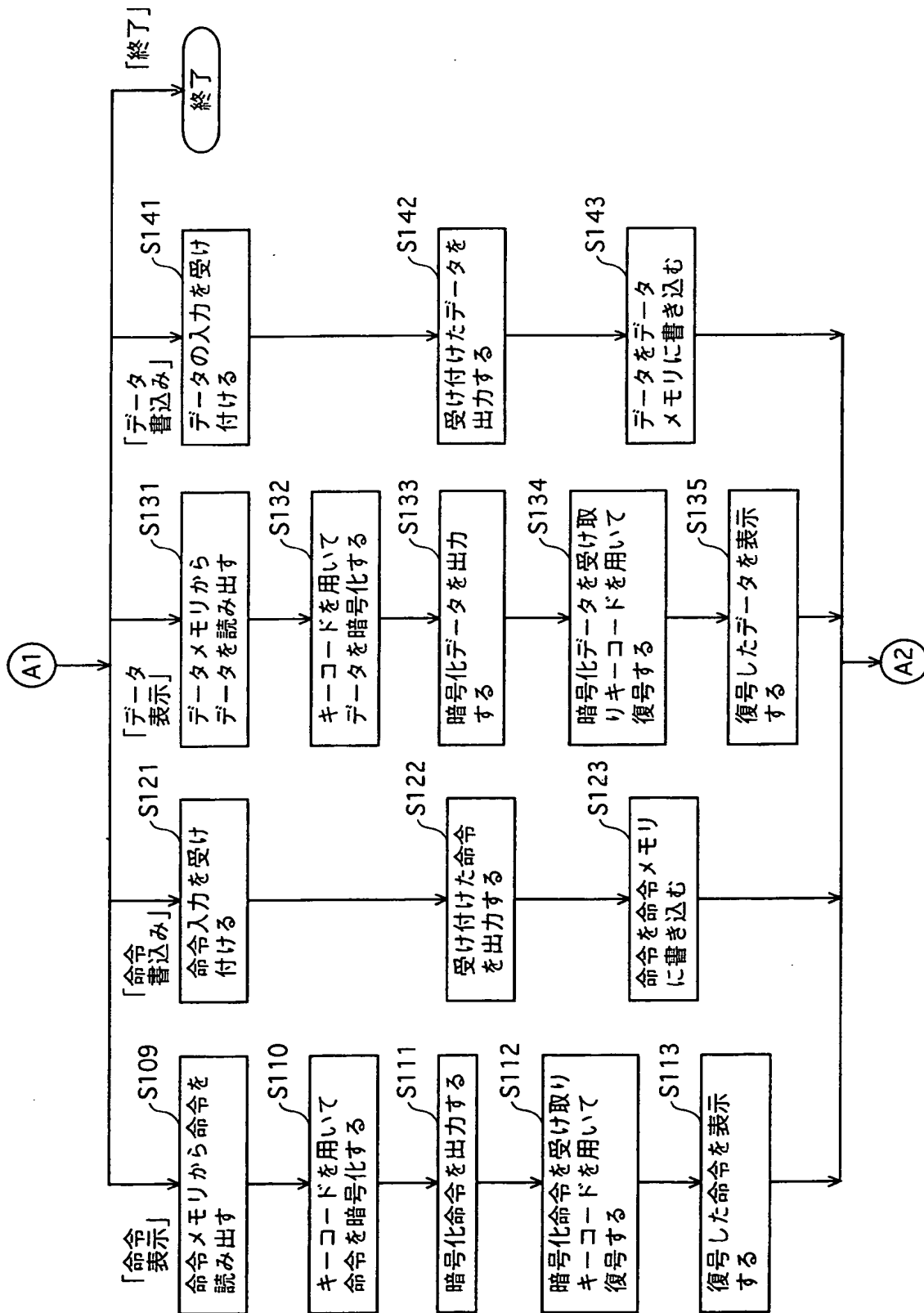
【図 2】



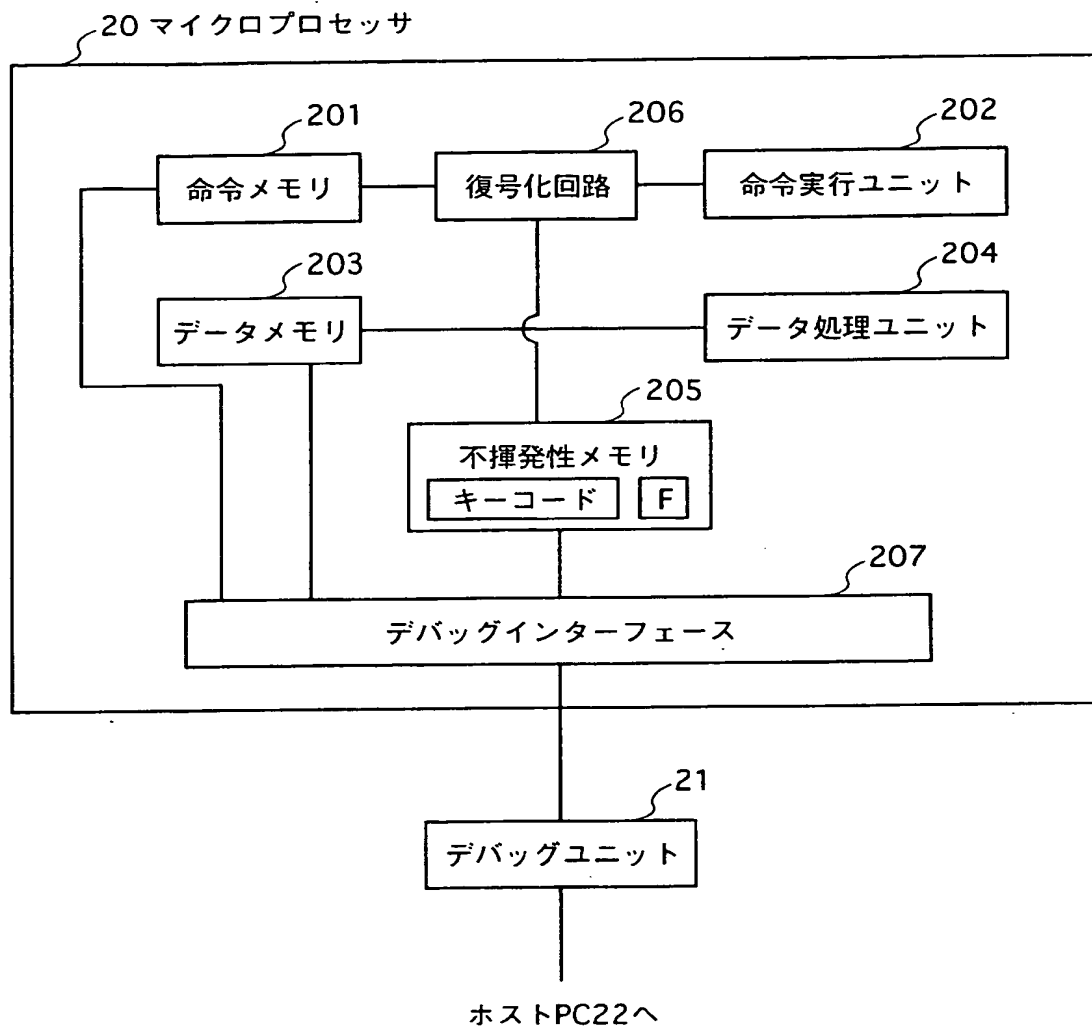
【図 3】



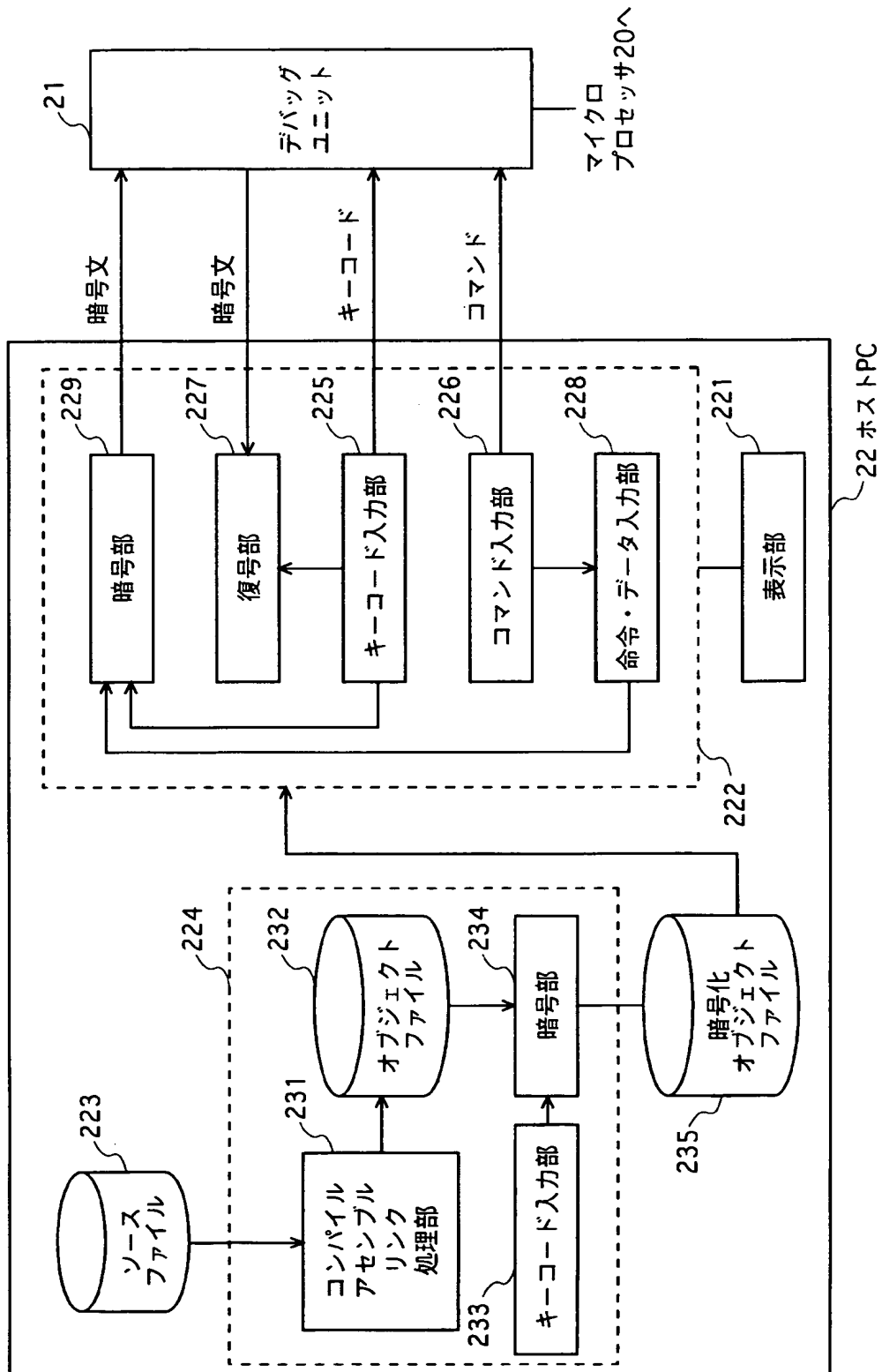
【図 4】



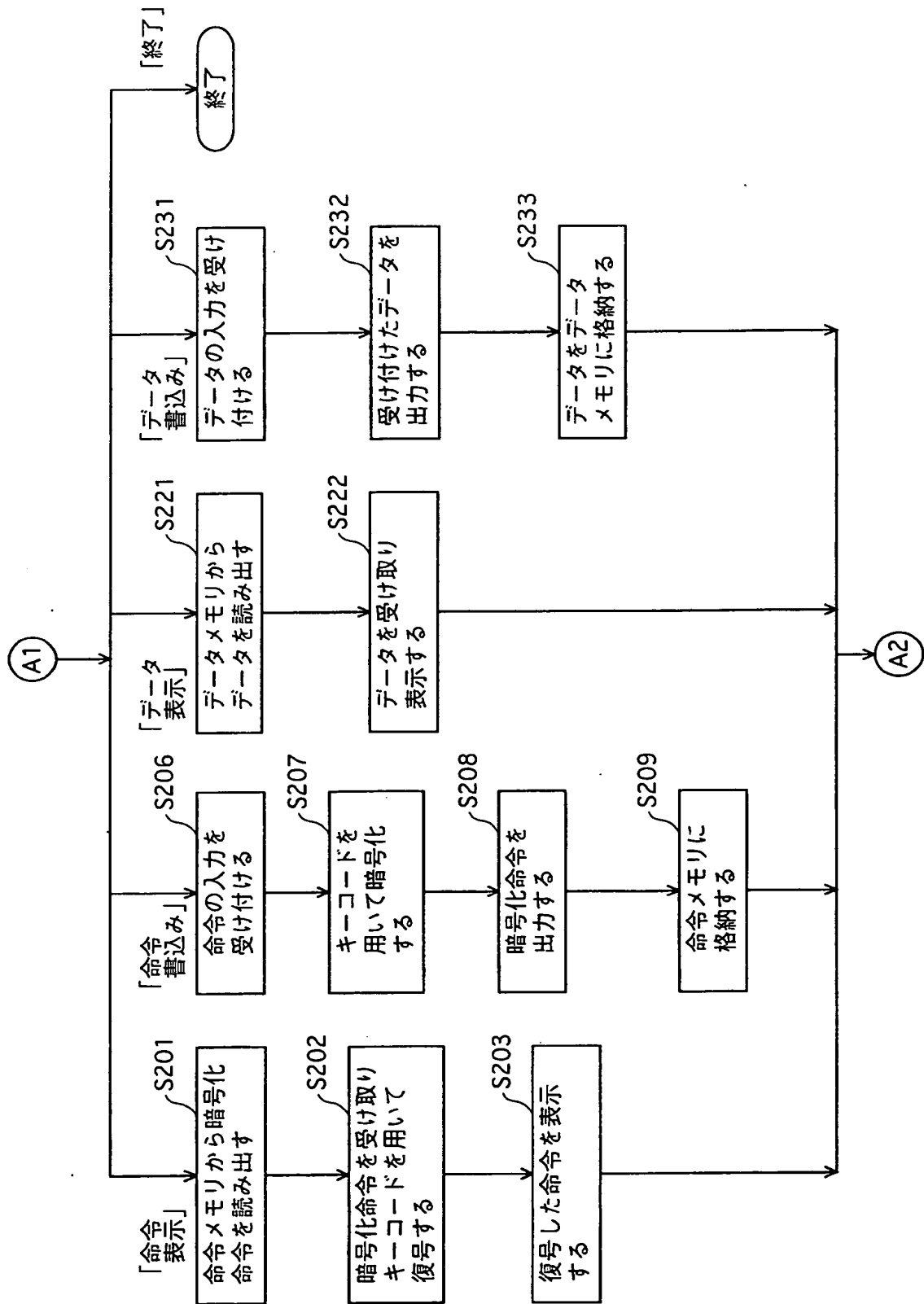
【図 5】



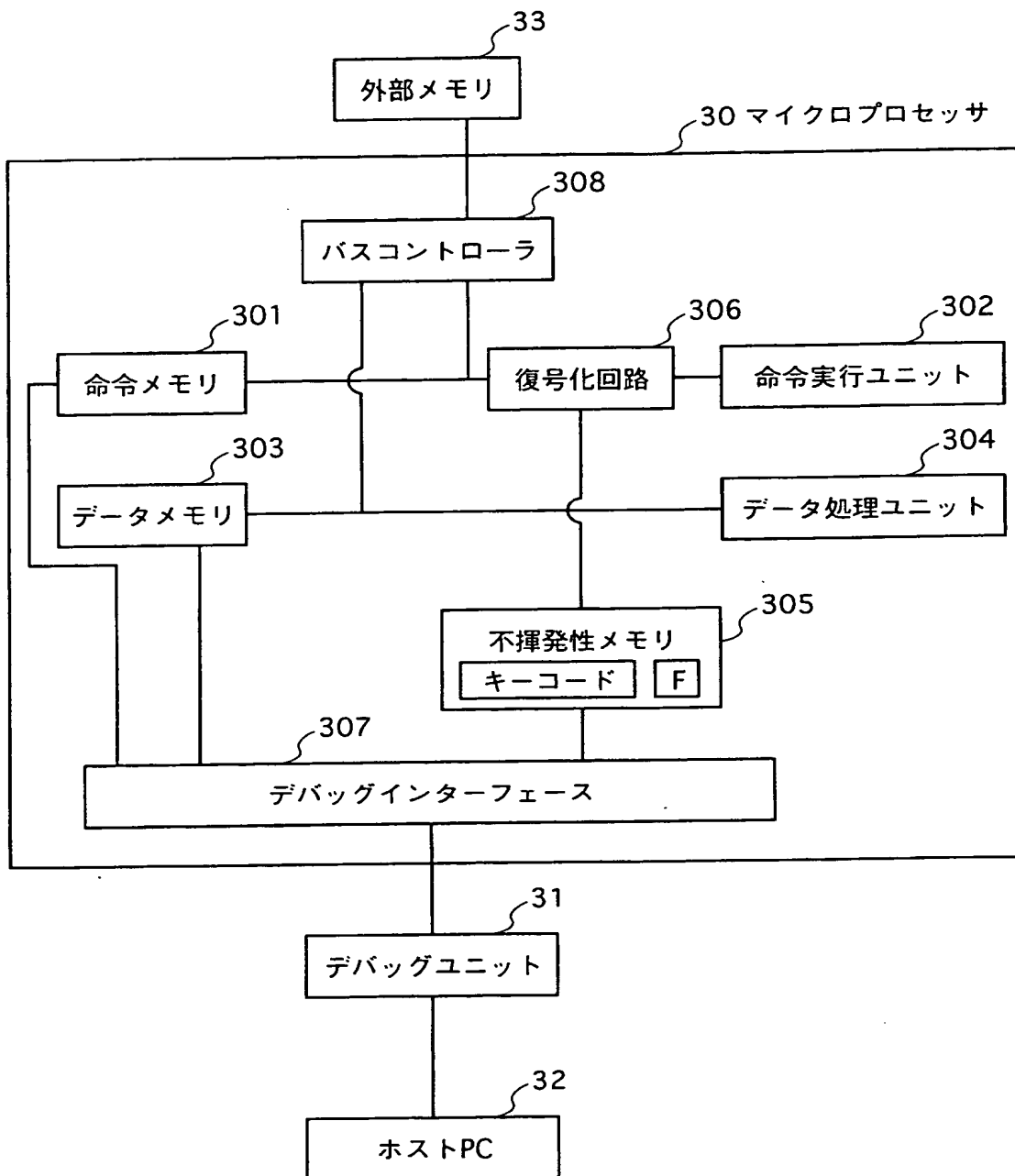
【図 6】



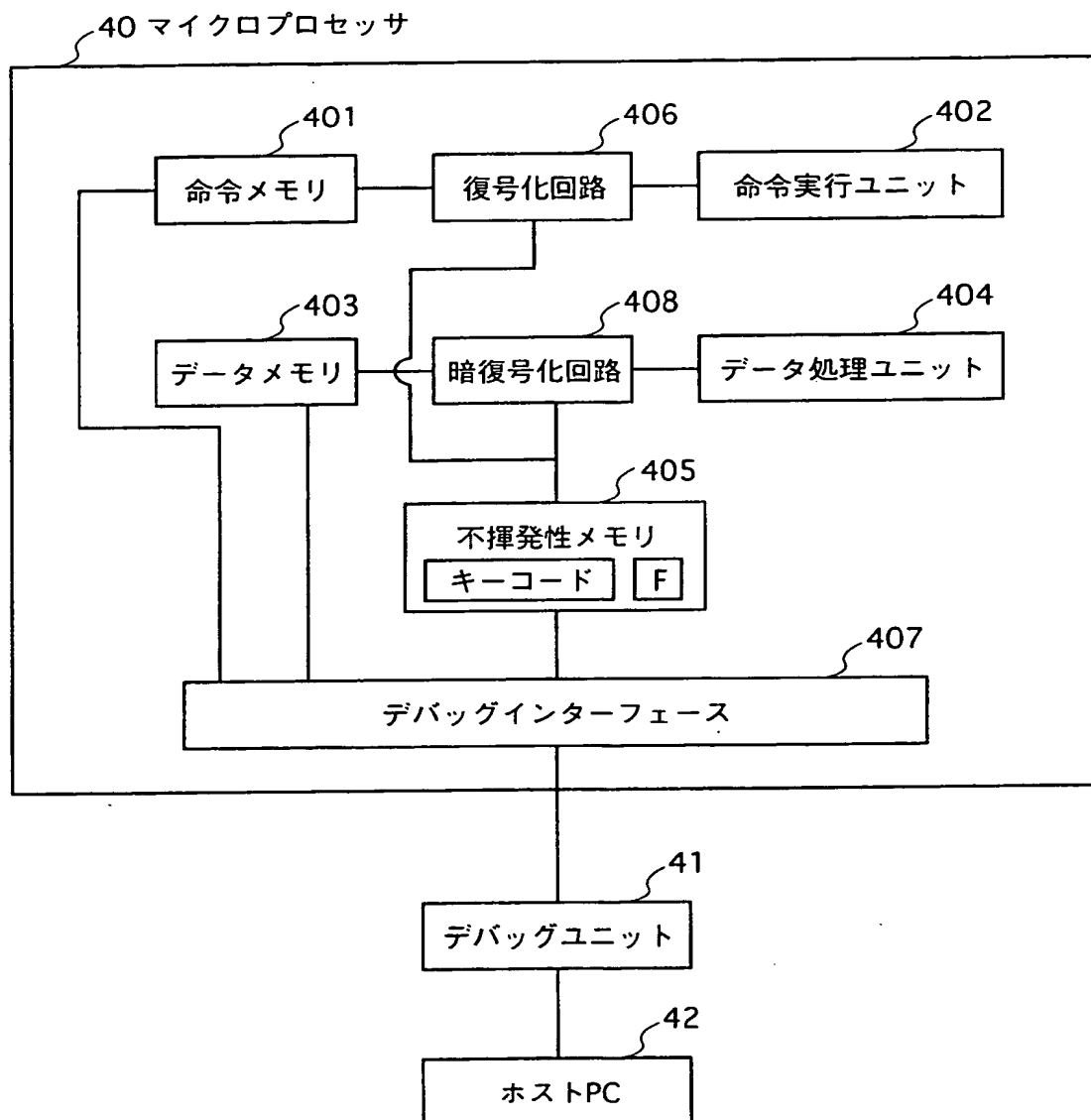
【図 7】



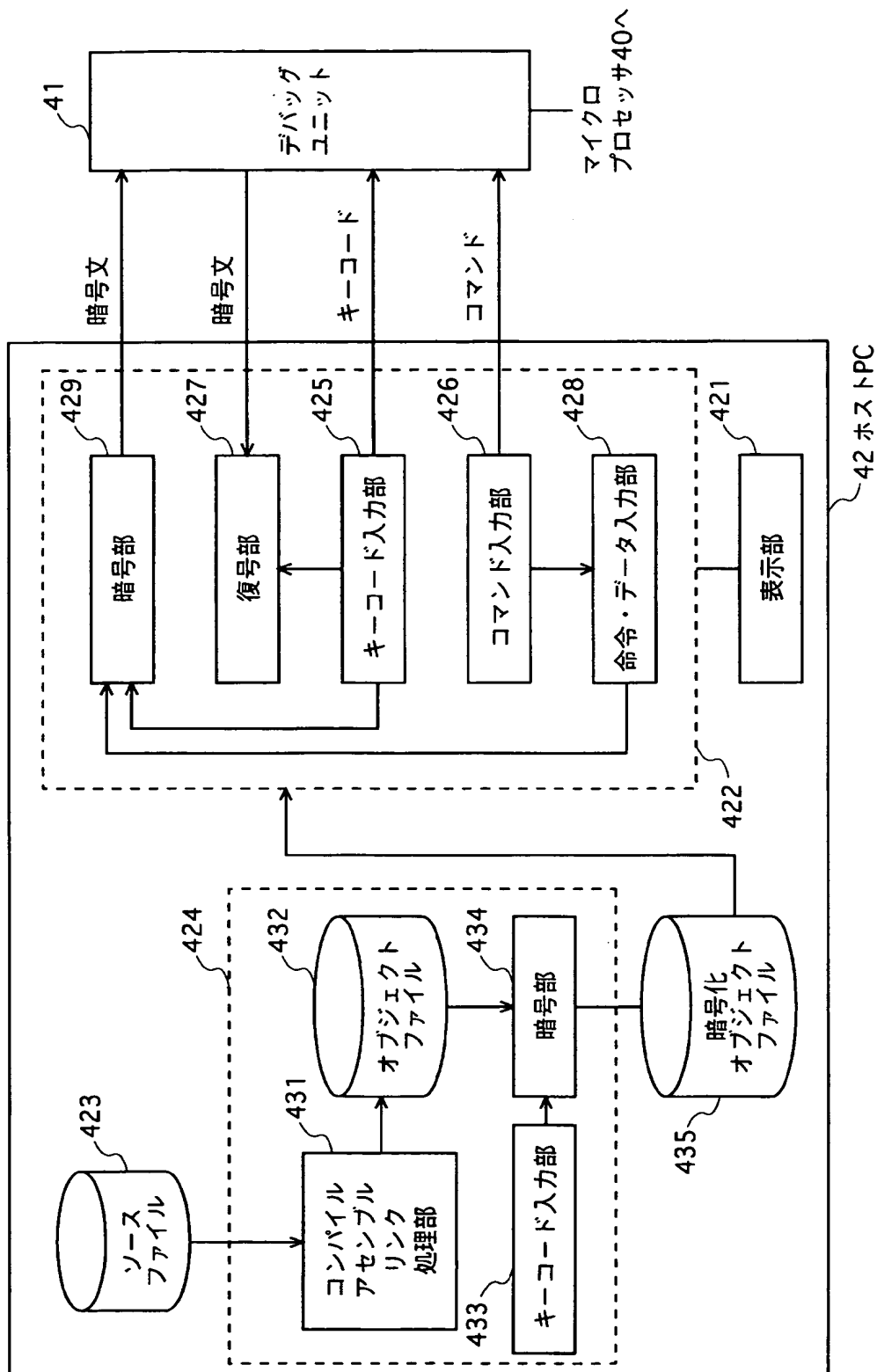
【図 8】



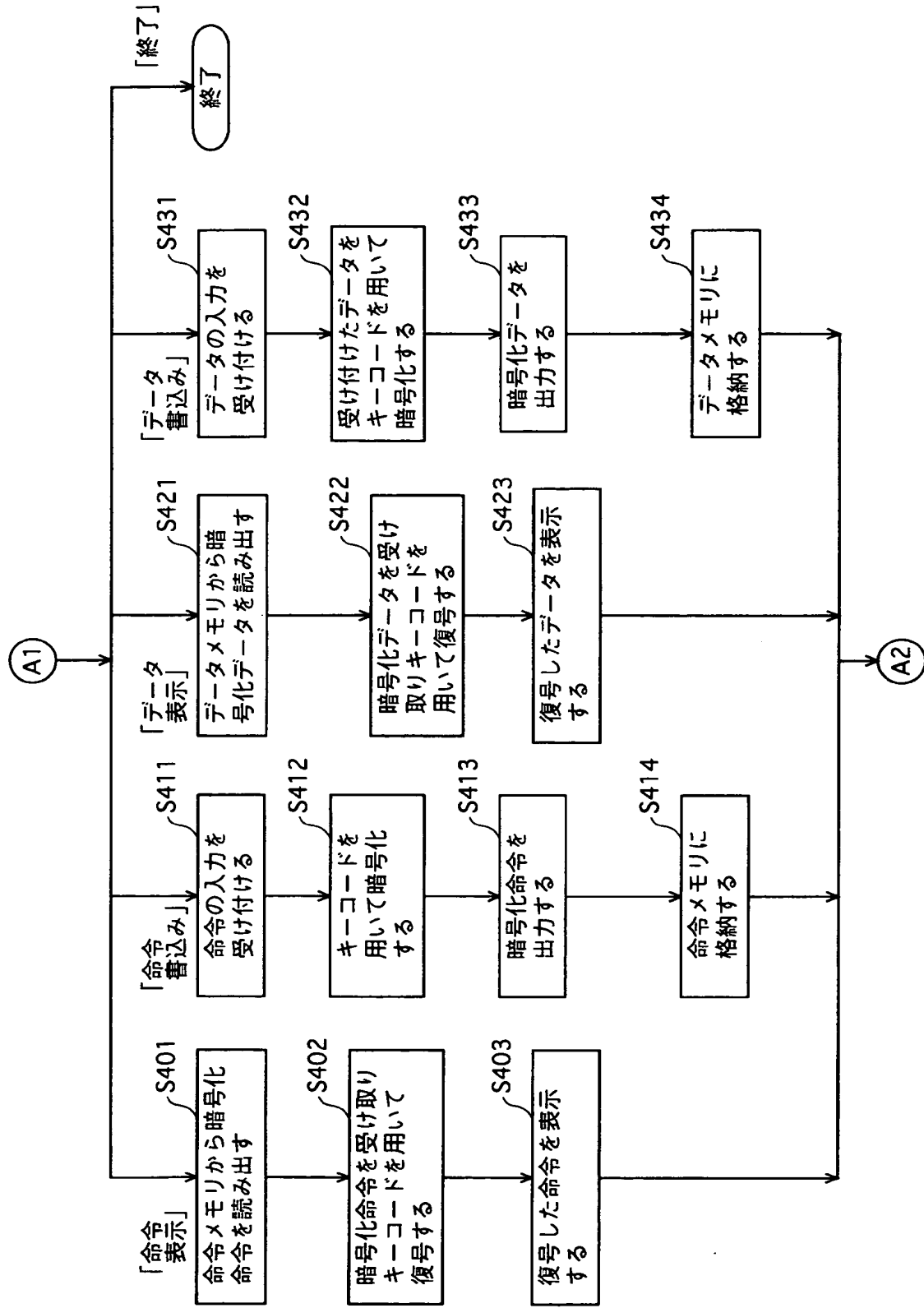
【図 9】



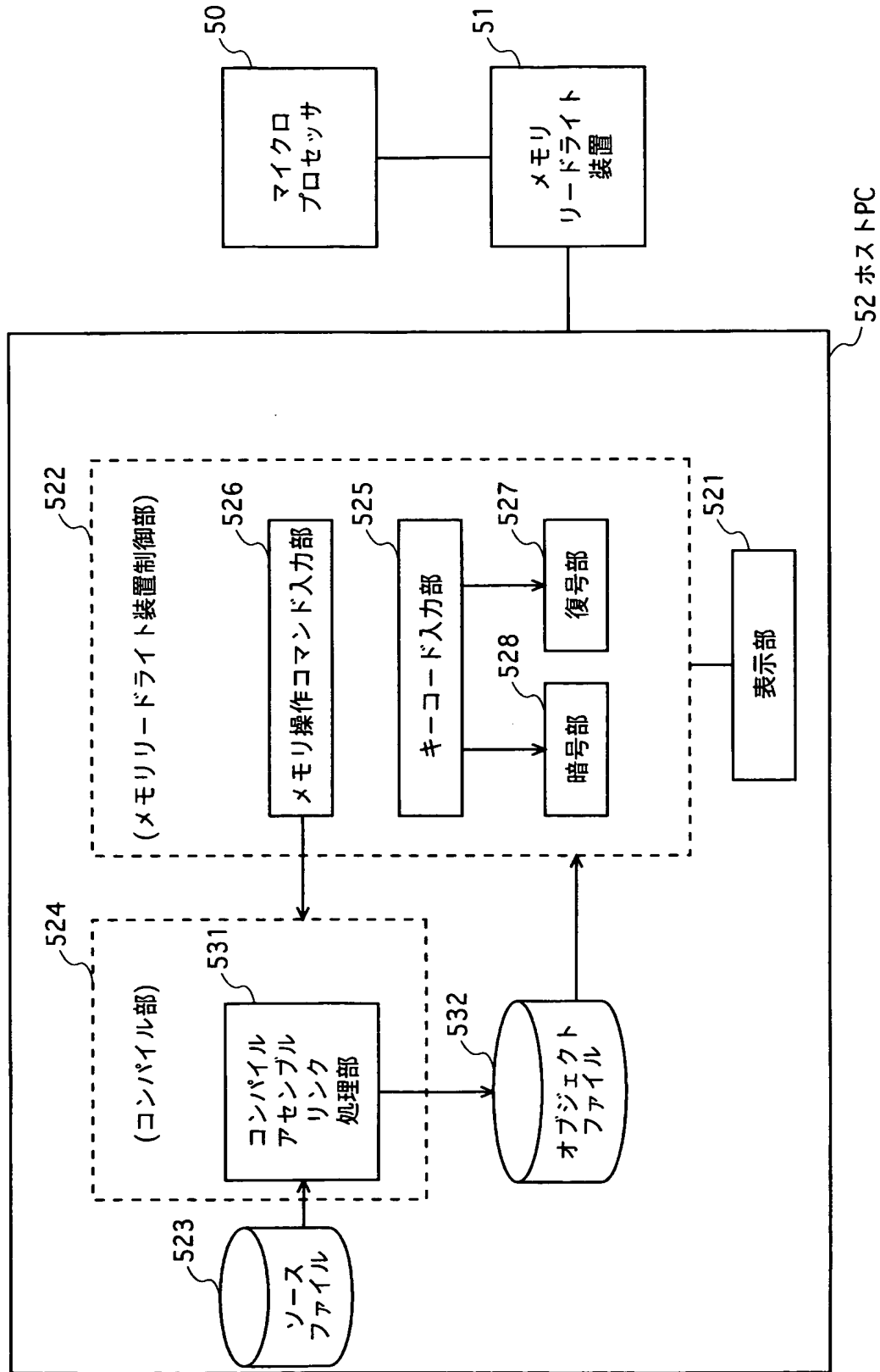
【図10】



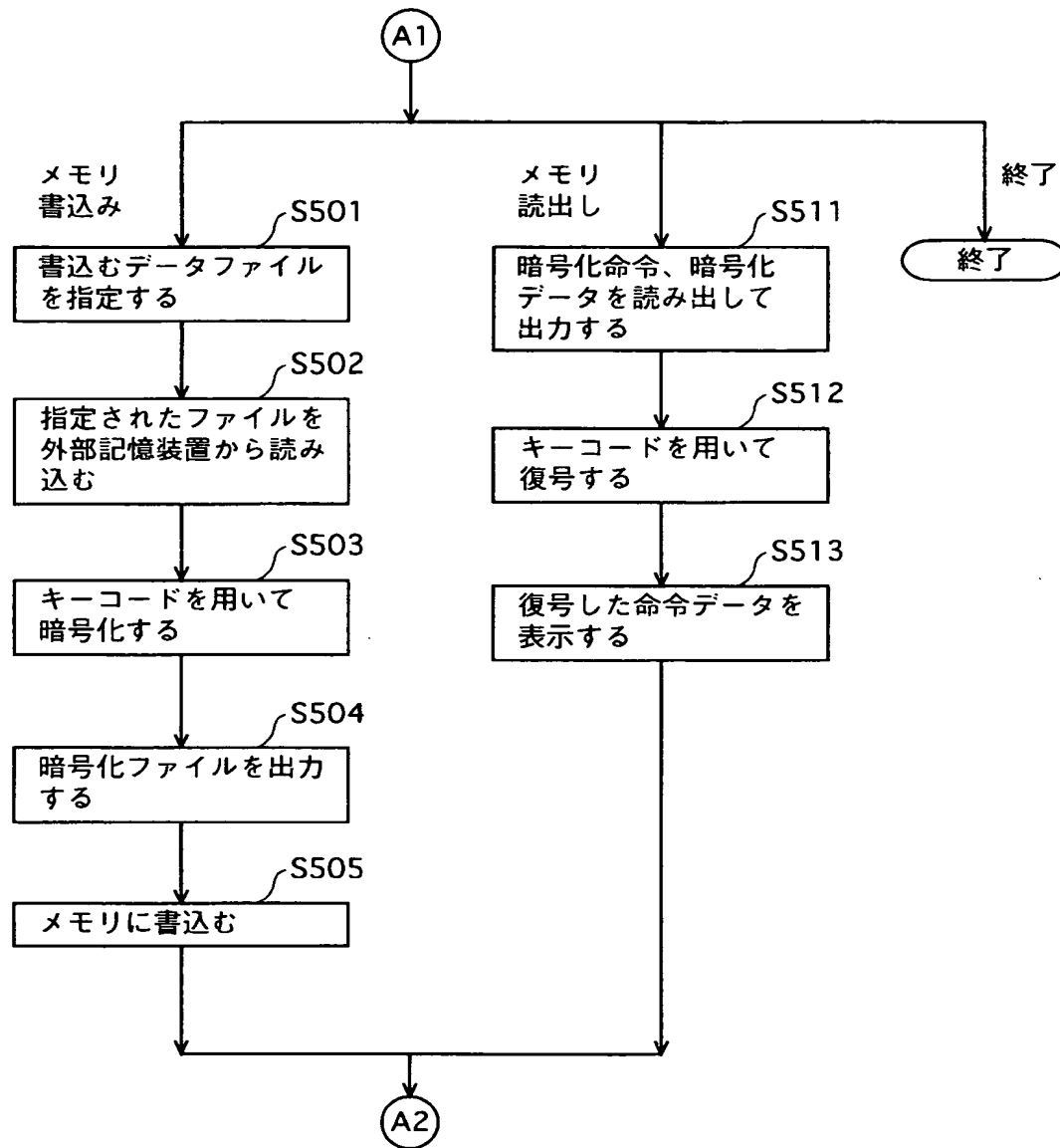
【図 11】



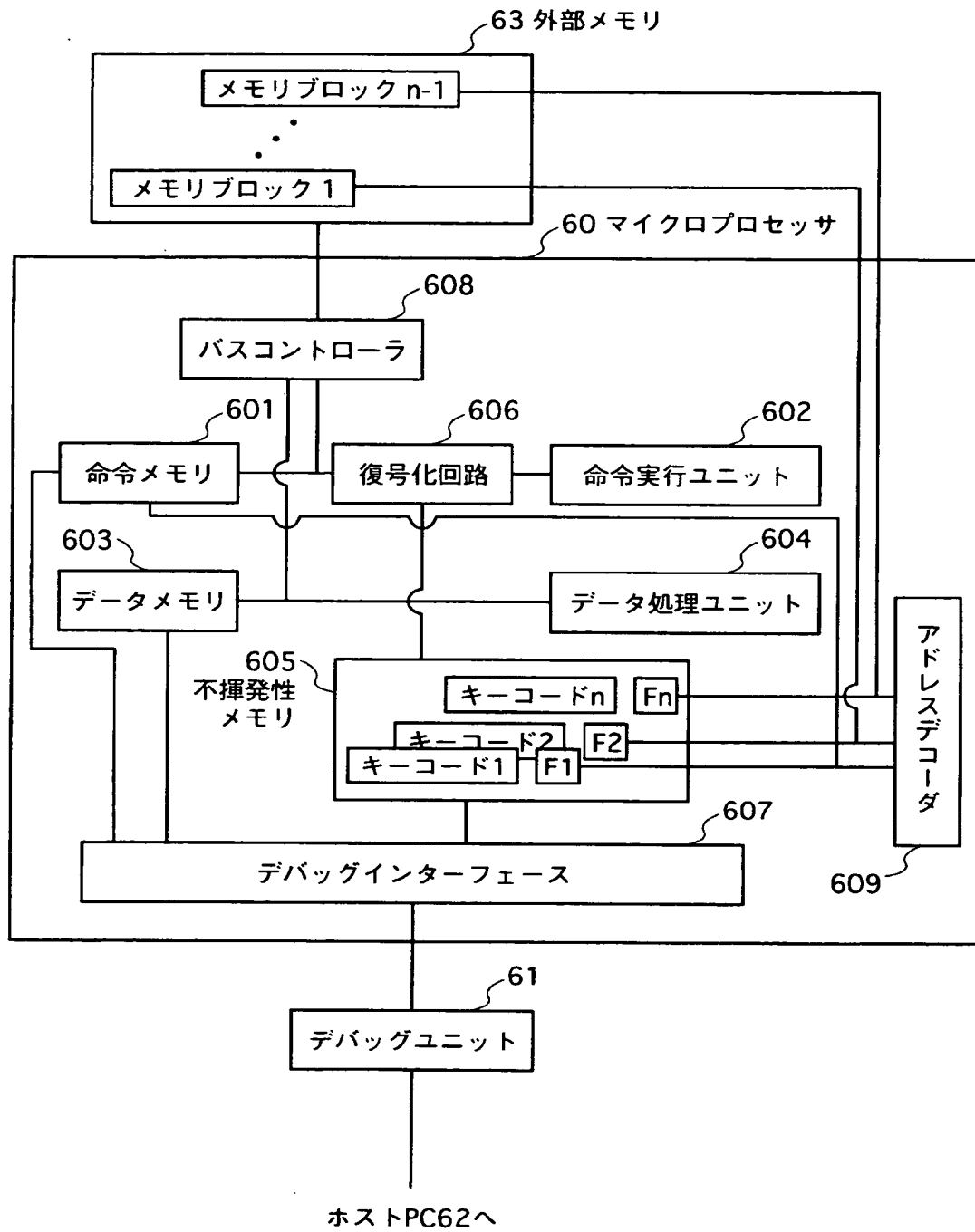
【図 12】



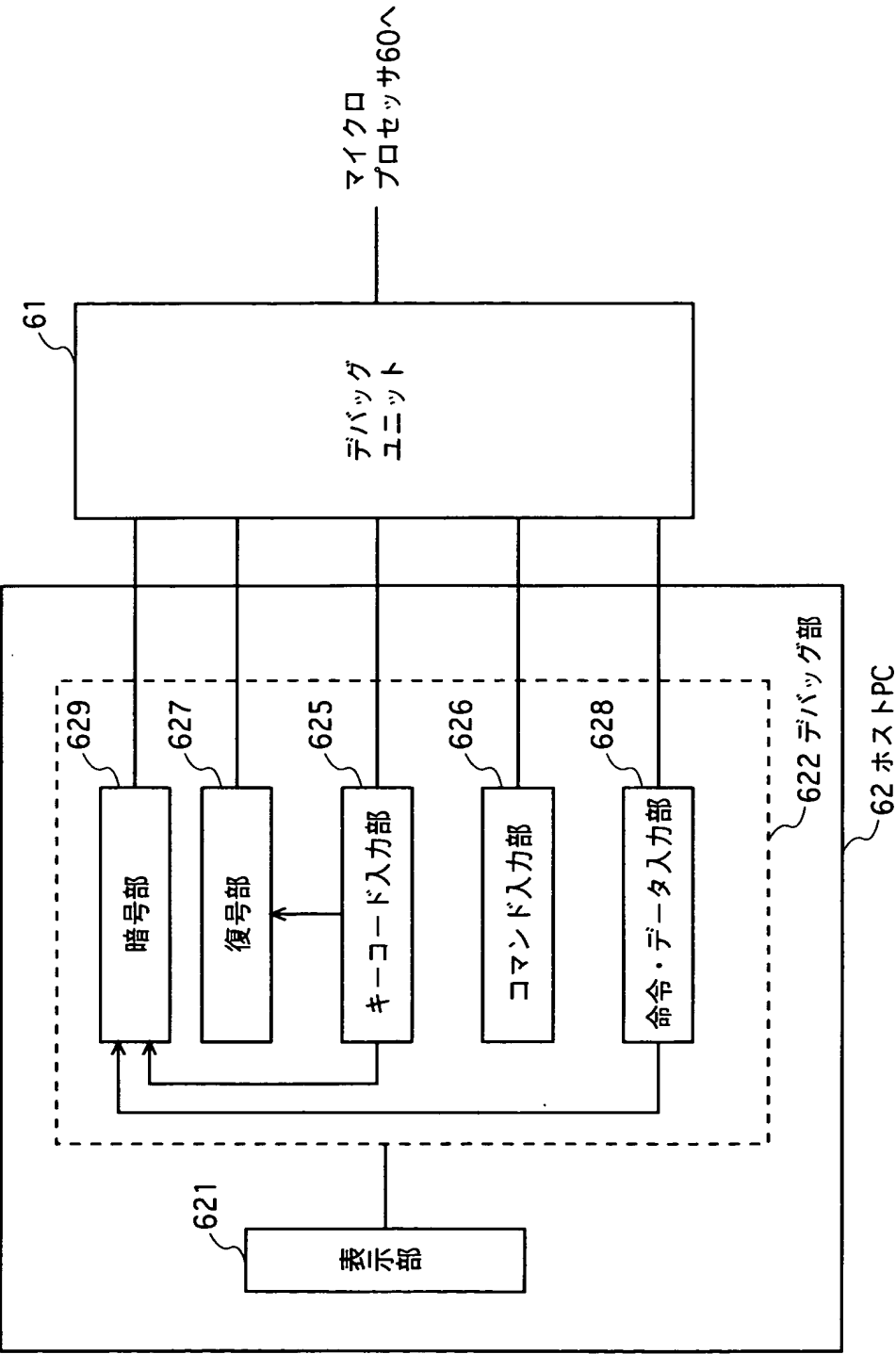
【図 13】



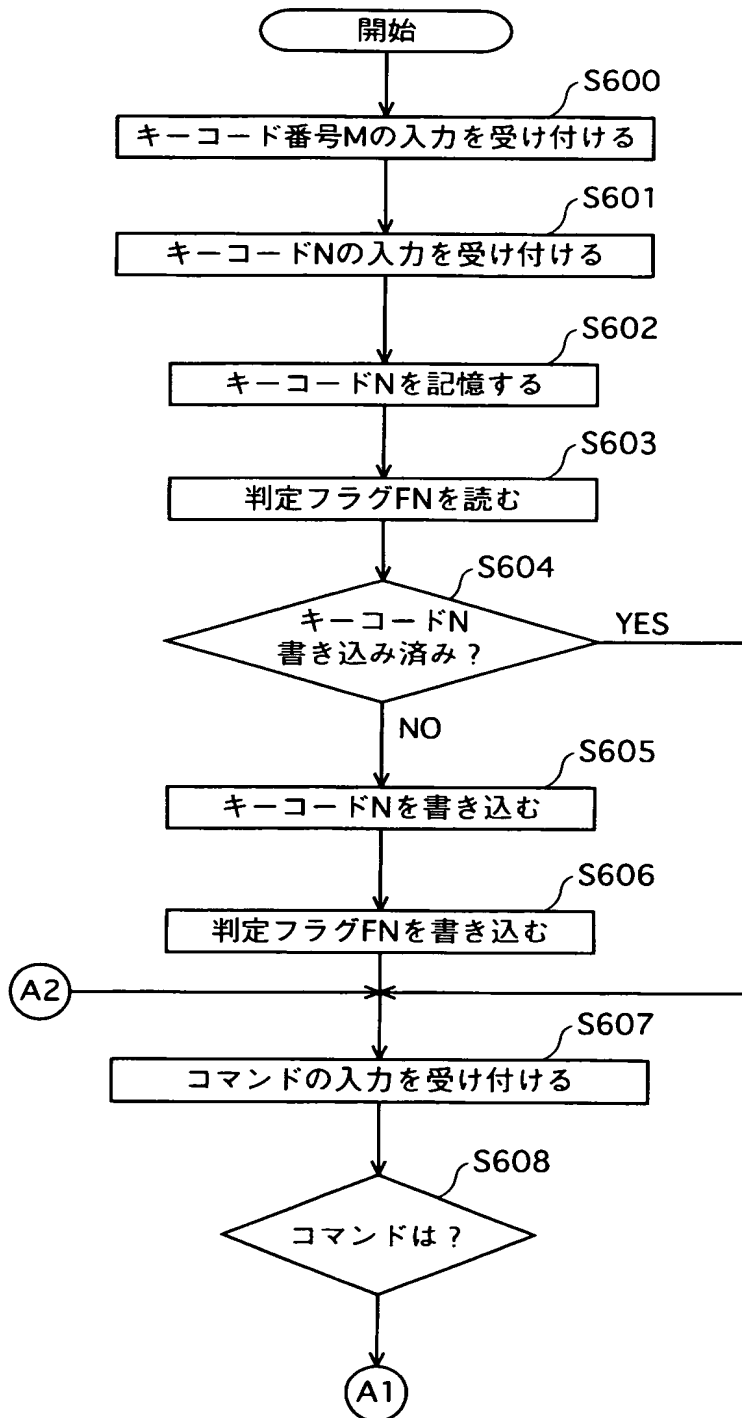
【図 14】



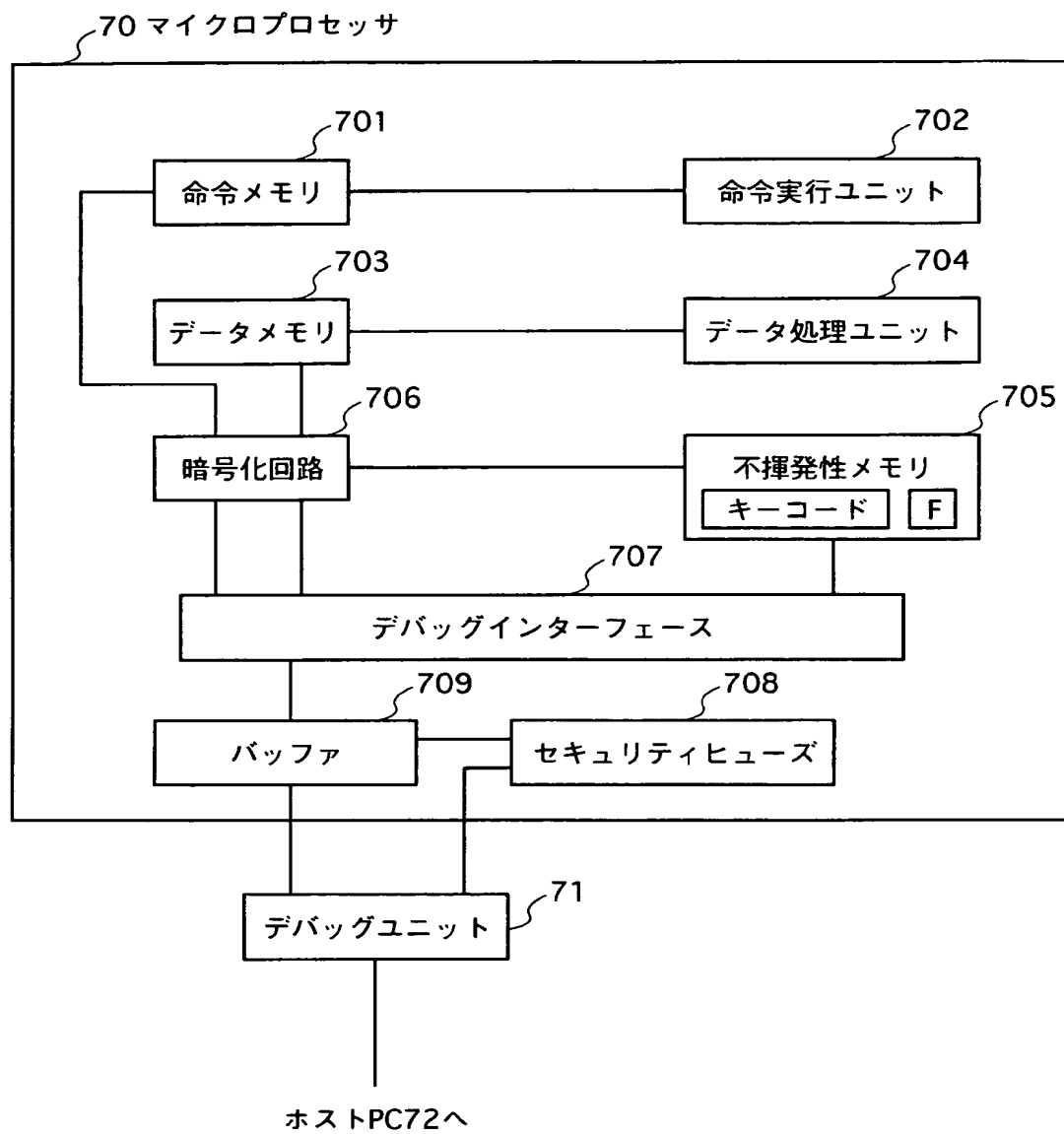
【図 15】



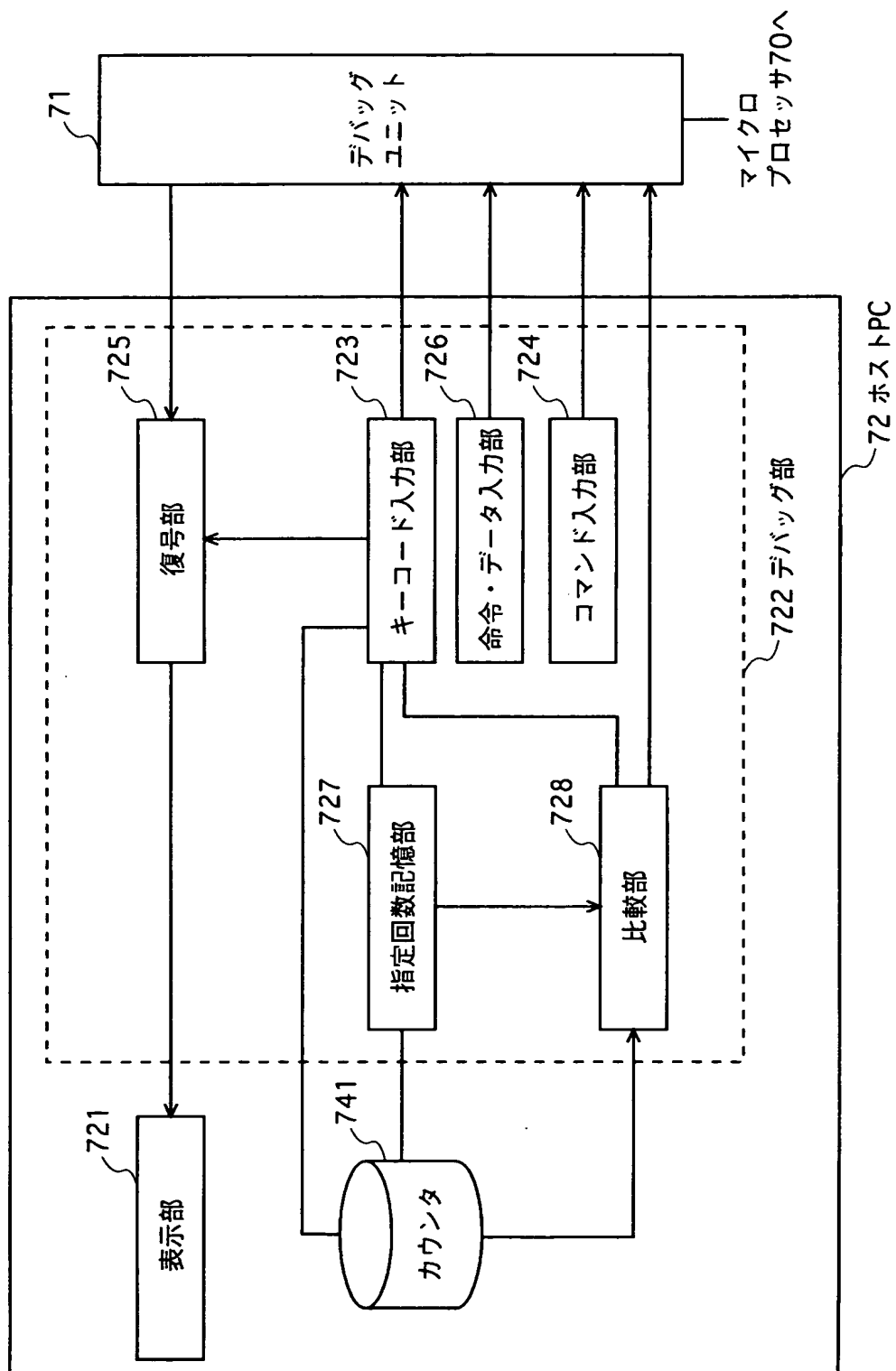
【図 16】



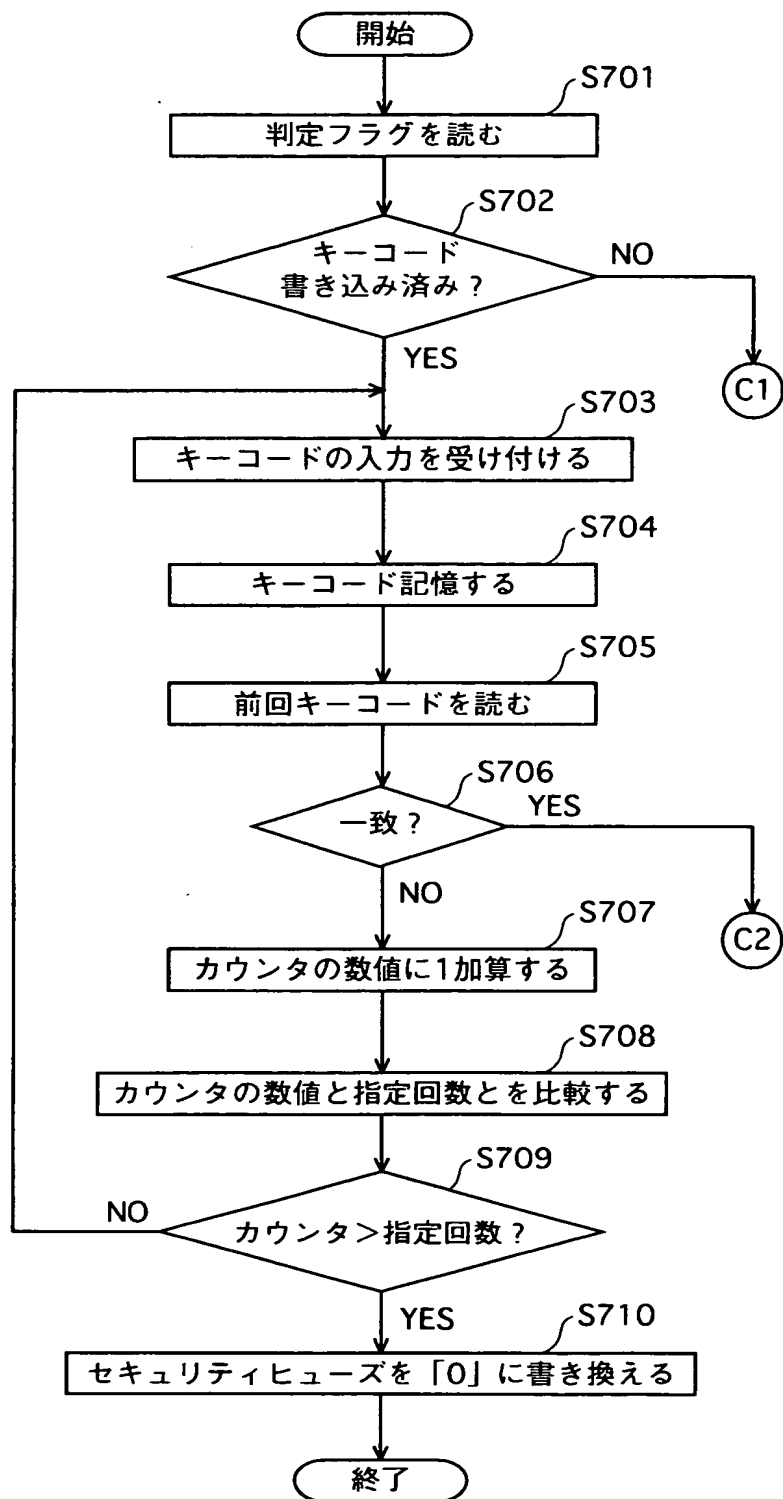
【図17】



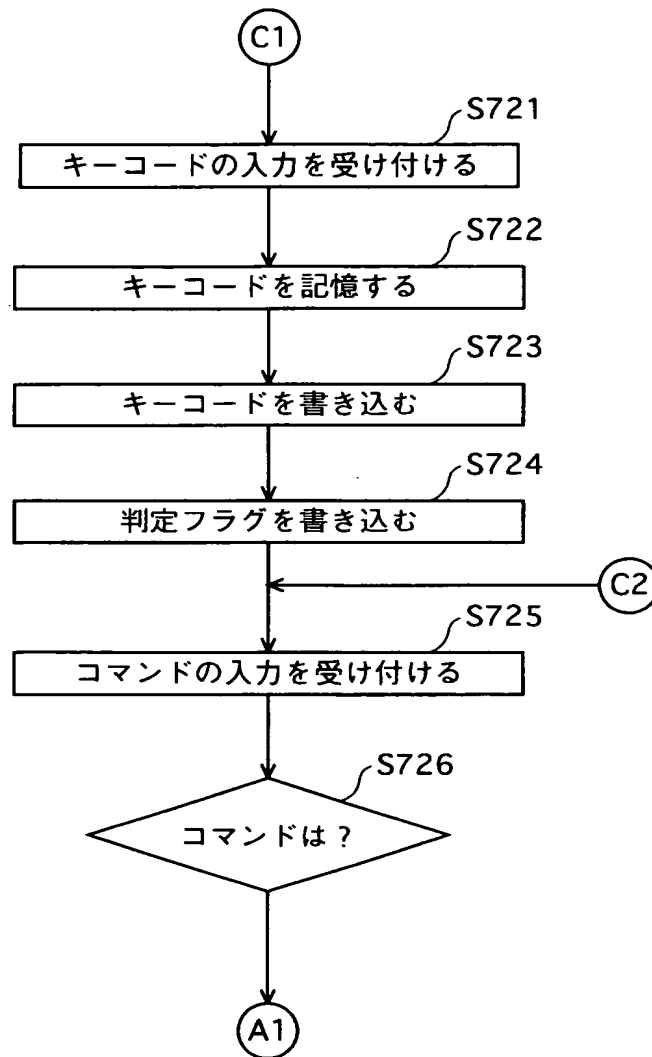
【図 18】



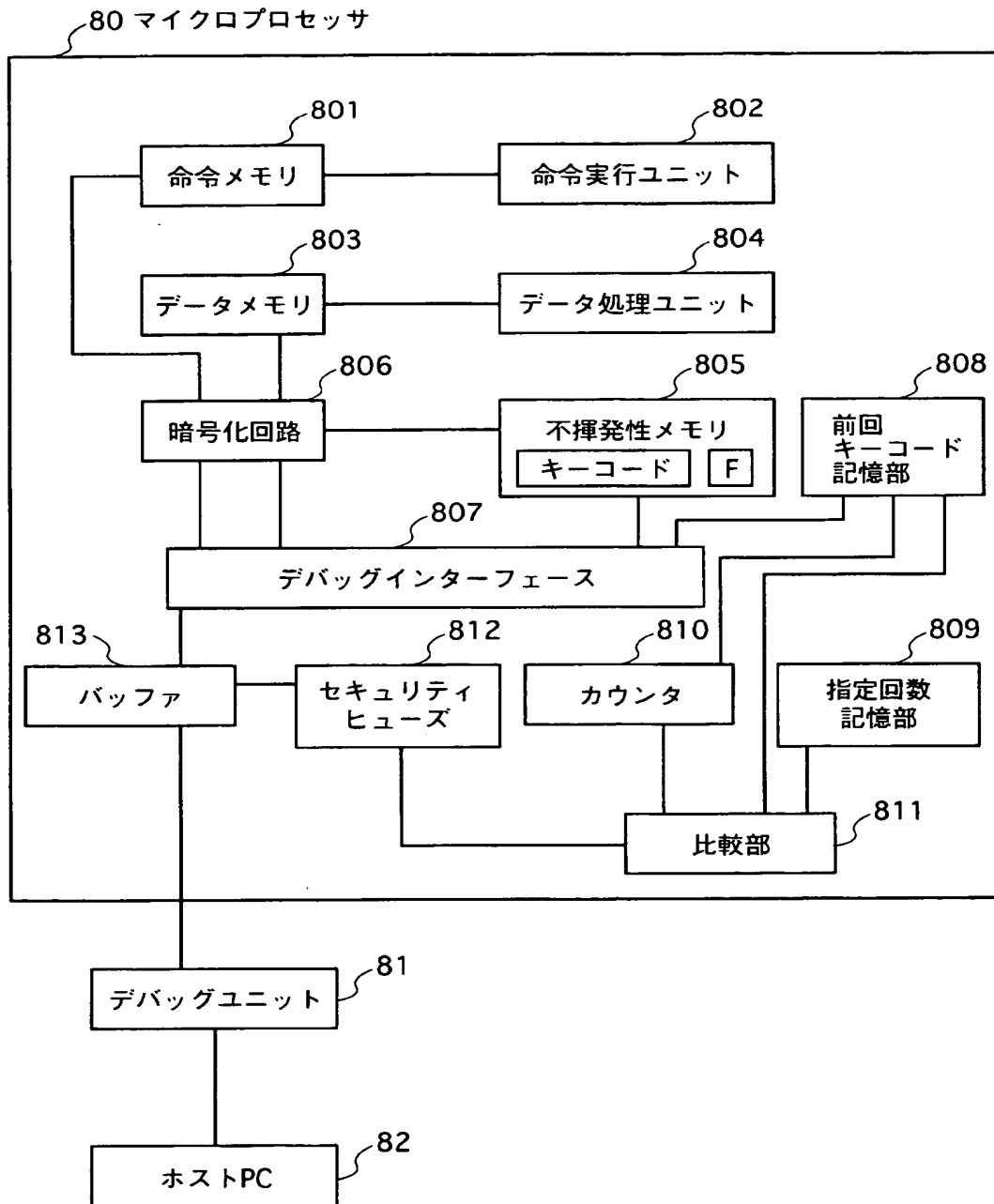
【図 19】



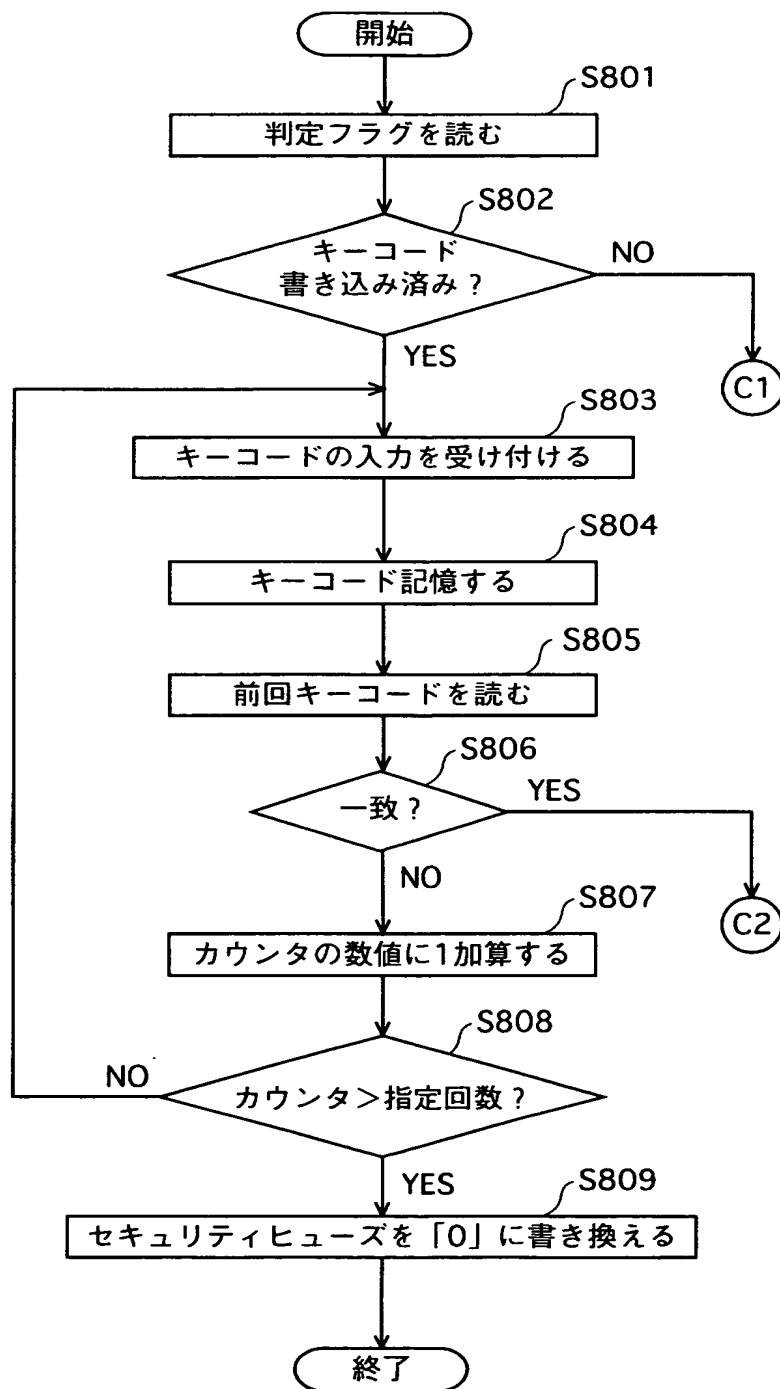
【図 20】



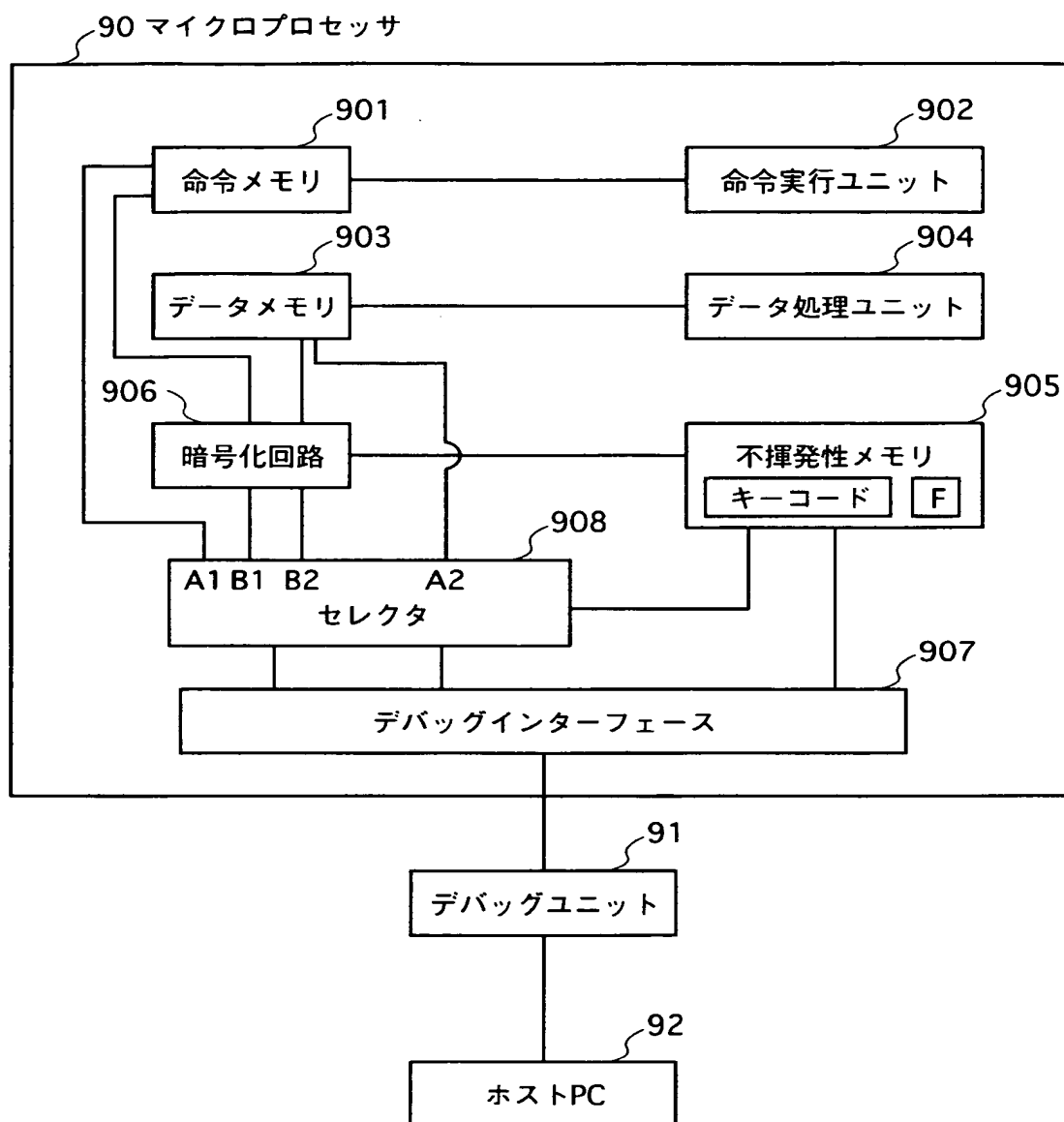
【図 21】



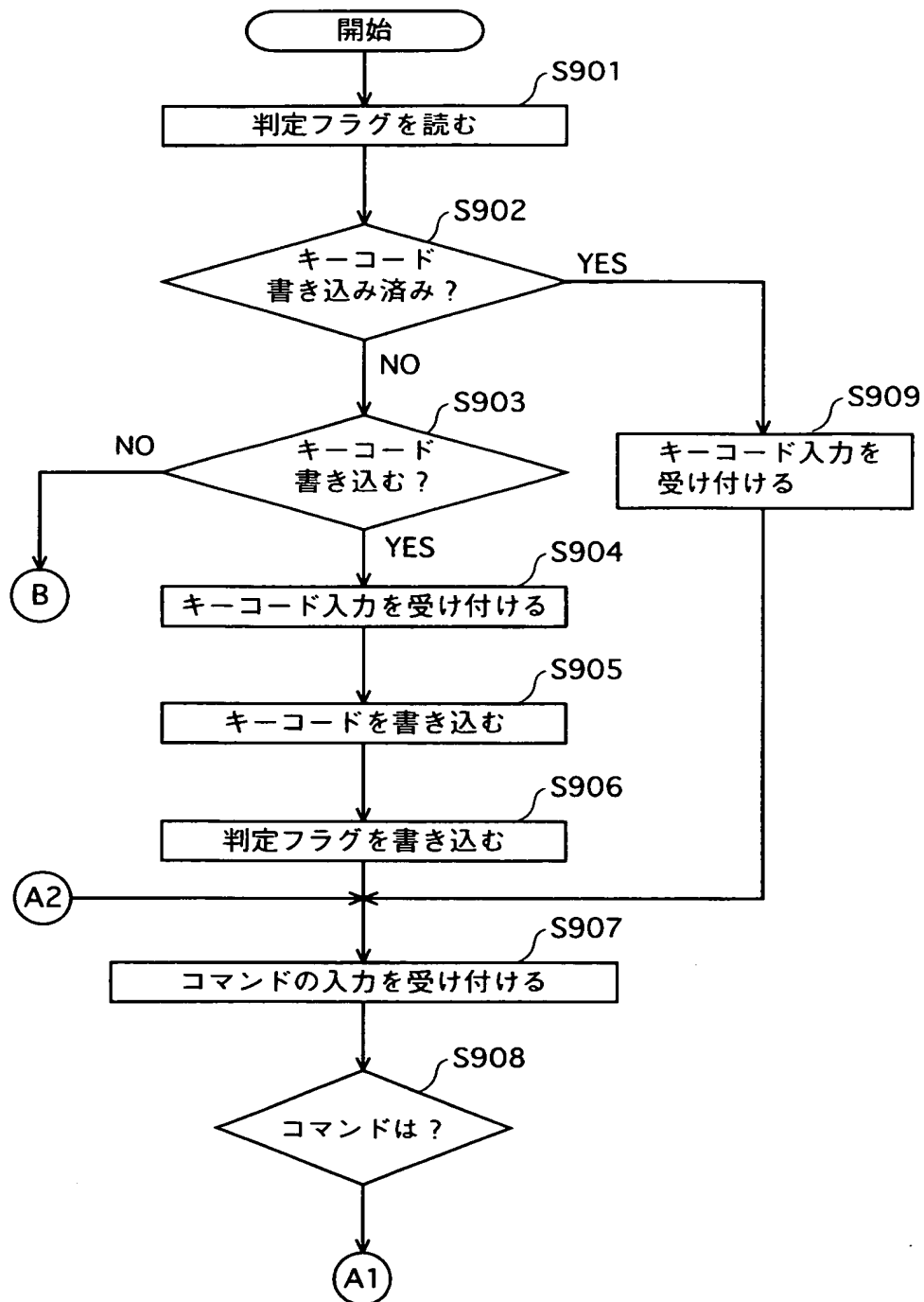
【図 22】



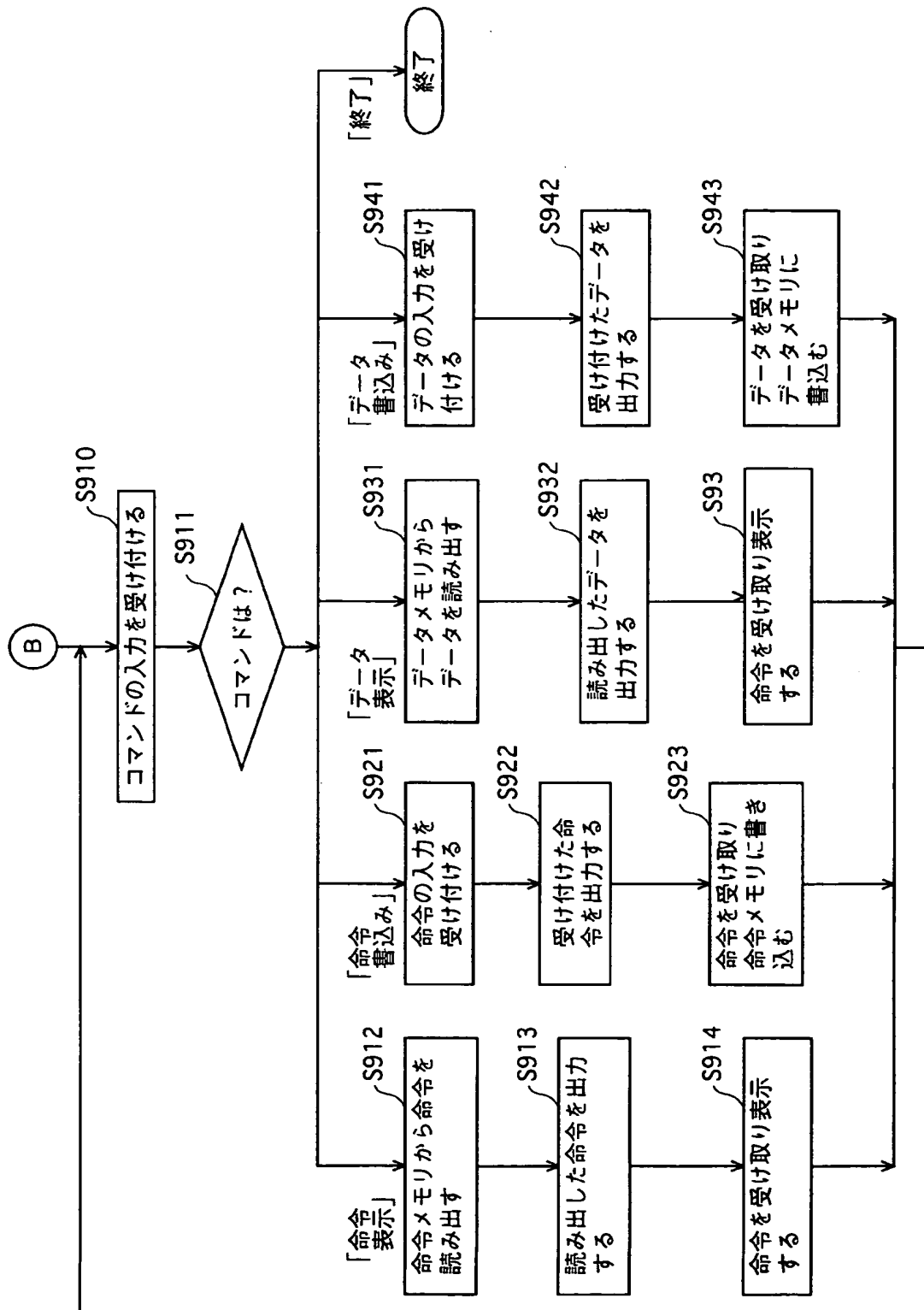
【図 23】



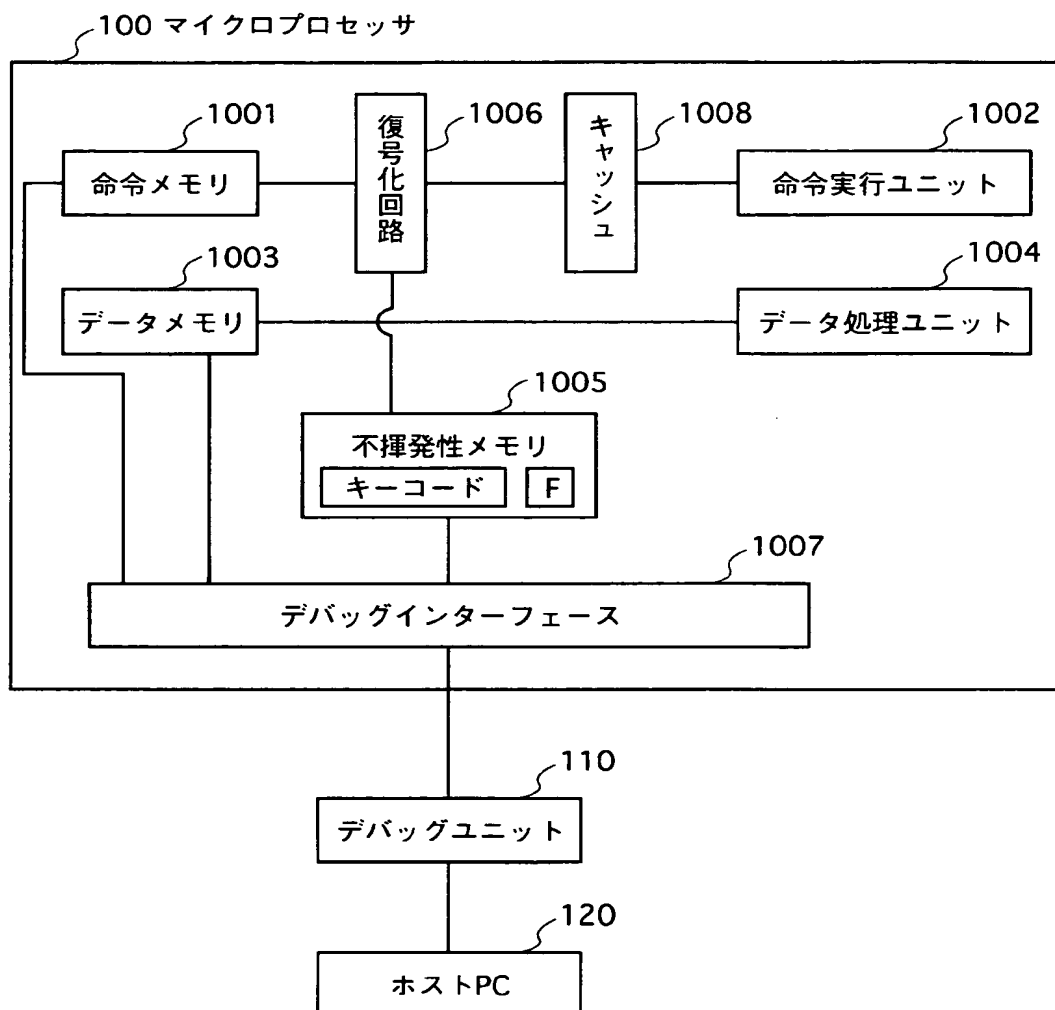
【図 24】



【図 25】



【図 26】



【書類名】 要約書

【要約】

【課題】 マイクロプロセッサのデバッグと内部情報のセキュリティの維持とを両立するデバッグシステムを提供する。

【解決手段】 マイクロプロセッサは、ホストPC上でユーザから入力されたキーコードを内部に記憶し、当該キーコードを用いて命令やデータを暗号化してホストPCへ送出する。悪意のあるユーザが、マイクロプロセッサをデバッグユニットに接続して暗号化命令及び暗号化データを取得した場合であっても、前記キーコードを知らなければ暗号化命令及び暗号化データを復号することはできない。

【選択図】 図1

特願 2 0 0 3 - 0 7 6 1 4 5

出 願 人 履 歷 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1 . 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社